「資通安全法律案例宣導彙編」

第七輯

行政院國家資通安全會報技術服務中心 編印
中華民國98年12月

序

近年來隨著網路及資訊技術的快速成熟，使得資訊相關應用也邁入一個新的境界，例如倍增的電子商務交易、網路訂位訂票及資訊系統支援的行銷活動等，都讓人們的生活變得更加的便利，但隨之而來的資訊安全議題也更加嚴重。因應這些變化，我國政府一方面不斷地增加或調整法令法規，例如：電腦處理個人資料保護法的修訂、針對金融公司使用客戶資料所制定的「金融控股公司子公司間共同行銷管理辦法」，及針對保護病人隱私之「門診醫療隱私維護規範」等，以期增加對民眾的保障。另一方面也成立「行政院國家資通安全會報」，除協調各部會落實資通安全施政優先項目外，並以實際行動強化資安法治觀念，強化政府部門對資通安全重要性之意識及認知。

「行政院國家資通安全會報技術服務中心」（以下簡稱技服中心）自 *91* 年起已發行 *6* 輯「資通安全法律案例彙編」。此彙編透過對相關案例的分析與學習，幫助政府部門及社會大眾建立網路環境應有的法治概念及安全意識，並進而達成預防網路犯罪之目標。在「技服中心」舉辦的各類資安宣導與推廣訓練活動中，此彙編之推廣發行普獲好評，政府機關(構)爭相索取運用，使「技服中心」深感持續推動此項工作之重要性。此次 *99* 年編印之第七輯「資通安全法律案例彙編」，持續委由「國巨律師事務所」蒐集近一年來發生之資安時事新聞與法院實際案例。內容除保持深入淺出的說明及專業法律觀點外，更進一步協請資訊安全管理顧問參照 *CNS27001*(資訊安全管理系統國家標準)之概念提供案例中各角色(如：公司與民眾等)管理及處理面的建議，以期增加對讀者的參考價值，相信此彙編必能成為政府機關及社會大眾學習資訊安全管理時最佳之參考教材之一。

行政院國家資通安全會報技術服務中心

劉培文主任　謹識

編 者 序

「資通安全法律案例宣導彙編」在「行政院研究發展考核委員會」(以下簡稱「行政院研考會」)與「行政院國家資通安全會報技術服務中心」(以下簡稱「技服中心」)共同推廣下，已然邁入第七輯行列。

本次延續第六輯的體例之編排方式，將資訊安全以「資訊保護」、「資訊公開」、「資訊監察」及「資訊應用」為類型，此外也有些許的改變，目的是提供讀者更親近的閱讀與更廣泛的學習素材。主要是在「資訊保護」增加醫療法規如醫師法有關的資訊保護案例與在「資訊公開」增加檔案法方面的案例報導。

在「管理 *Tips*」，除了延續摘要 *CNS27001*（資訊安全管理系統國家標準）附錄 *A* 作為個案管理標準外，也同時以口語化方式表達管理建議，讓讀者瞭解管理顧問對於個案解析的內容，藉此作為自我審查的參考意見。此部分是請資誠企業管理顧問股份有限公司蔡興樺協理協助說明。

在本次選擇的 *30* 則案例中，包含了 *18* 則「資訊保護」相關的案例，是彙編中最主要的範圍，「資訊公開」與「資訊監察」則各有 *3* 則，而「資訊應用」則有 *6* 則。這些案例內容對於時下的個人資料保護、監聽他人通訊及線上法拍都提供值得參考的法律訊息。

值此資訊安全日益重視的年代，政府亦提倡使用雲端運算服務，對於資訊安全基礎的法治教育也更顯重要。藉由法律案例的解析，讓政府與民間部門在資訊安全科技工具的選擇外，也增添行為規範的準則，讓整體社會資訊流通朝向正面發展。

國巨律師事務所
朱瑞陽律師謹識

凡　　例

壹、本案例彙編分為以下類別：

一、資訊保護 *(Security)*

01 電腦處理個人資料保護法

02 國家機密保護法

03 營業秘密法

04 刑法

05 醫療法規

二、資訊公開 *(Disclosure)*

01 政府資訊公開法

02 檔案法

三、資訊監察 *(Monitors)*

01 通訊保障及監察法

四、資訊應用 *(Application)*

01 電子簽章法

貳、本案例編碼共 *7* 位數字：編碼方式以上述四大類別之英文字首為第一碼，再加上年份及上述各小類之編碼各兩碼，最後兩碼為該小類中之第幾篇案例。例如：*S980101*，即代表資訊保護類 *98* 年度之電腦處理個人資料保護法第一則案例。

目　　次

壹、　資訊保護（*Security*）.....1
一、 電腦處理個人資料保護法.....2
人肉搜索　波蘭醫師背景網路大公開.....2
洩漏考生資料　每筆資料判賠 *100* 元懲罰性違約金.....5
戶籍謄本列印新制　婚姻紀錄可不曝光.....8
Facebook 流量增加　面臨資料外洩之威脅.....12
採集生物檢體應行告知程序並予以保密.....15
機場電腦故障　境管門戶洞開.....19
防個資外洩　別填身分證字號.....23
勾結員警盜賣個資　檢方起訴不法集團.....27
二、 國家機密保護法.....30
拍攝資電中心　陸客誤入不起訴.....30
三、 營業秘密法.....33
離職員工借密碼　遠銀安泰打官司.....33
離職員工偷機密　與老東家削價競爭.....37
四、 刑法.....42
怕被打壓開會錄音，被檢方起訴.....42
戶籍資料不慎外洩　戶政事務所課員遭起訴.....45
製作山寨版人事局網頁　以偽造公文書送法辦.....49
台哥大跨年當機　工程師搞鬼.....52
竊飛彈資料　技術員涉貪污.....56
購物網站標錯價　疑遭駭客入侵.....59

五、 醫師法 64
洩露病人減重　醫師被罰 64
貳、 資訊公開（*Disclosure*） 68
一、 政府資訊公開法 69
法官評鑑委員會會議紀錄非屬應公開之政府資訊 69
公文承辦人姓名屬於限制公開或得不予公開之資訊 72
二、 檔案法 74
國家機密檔案朝全面開放修法 74
參、 資訊監察（*Monitors*） 78
一、 通訊保障及監察法 79
司法院：依法監聽　掛線僅 *6* 萬 79
都是開心農場惹的禍？中研院監控同仁電腦！ 84
杜絕違法監聽　刑事局查扣抓姦機 87
肆、 資訊應用（*Application*） 90
一、 電子簽章法 91
貨櫃電子封條取代人工押運 91
香港聯合醫院率先將病人資料上載至互聯網　減少遺失「手指」洩病歷 95
考生遭冒填志願　大學分發擬採自然人憑證 99
推廣工商憑證　經部估 98 年底達 92 萬張 102
衛生署加速實施電子病歷 105
黑道介入法拍屋　司法院擬修法防範 108

壹、資訊保護（*Security*）

一、電腦處理個人資料保護法

類別：資訊保護

【案號：*S980101*】

人肉搜索　波蘭醫師背景網路大公開

【資料來源：聯合報 *98/06/29*】

焦點話題

繼網路流傳波蘭醫學生回台考取住院醫師名單後，最近網路更貼出這些波蘭醫學生或醫師的家長，其中不乏知名醫師，連在哪家醫院任職都被公布，名單在網路上一再被轉寄，波蘭醫學生及家長不滿被「人肉搜索」，覺得隱私權嚴重被侵犯。

「波蘭醫師一覽表(*POPO OUT*)」部落格，開宗明義寫道：「提供波蘭醫師名錄給民眾就醫時參考，並歡迎大家透過電子郵件提供名單」，多名醫師均遭到點名，被點名的醫學生甲 *OO* 質疑：「針對我就好，為什麼要拉父親下水?」開業婦產科醫師乙 *OO* 有兩名兒子在波蘭習醫，女兒在台北醫學大學就讀醫學系也被寫出來，他不明白「為何連女兒都被扯進去」。

但名單中部份資訊的確有誤，台大醫院外科住院醫師甄選被拒的事件主角，一度被說成丙 *OO* 的女兒，丙 *OO* 澄清他只有兩個女兒，但都不是醫學系，他無奈表示不懂自己為何平白無故「多了一個女兒」?此項錯誤資訊已經被更正，且向丙 *OO* 致歉。

重點摘要

1. 個人行為目前雖然不是電腦處理個人資料保護法規範的適用主體，但蒐集資料若涉及他人隱私時，仍屬於侵害他人隱私權之行為。

2. 網路上發表言論必須要負責。

3. 行政院衛生署網站上可以查詢醫師執業資料。

法律觀點

「人肉搜索」是大陸網路詞彙，就是透過網友以「團結力量大」，由眾人將「人肉搜索令」鎖定之目標，透過網路搜索、個人人脈關係，甚至是剛好有人認識人肉搜索令的通緝犯，而將標的各項資料拼湊出來。進行人肉搜索涉及公開個人資料，除了侵害個人隱私權外，更有可能妨害他人名譽。

此案例涉及網友搜尋並公布就讀波蘭醫學生的資料會不會違反電腦處理個人資料保護法。波蘭醫學生的姓名、家庭、教育及職業均是電腦處理個人資料保護法定義之個人資料範疇[1]，但因現行電腦處理個人資料保護法適用的非公務機關限於特定的八種行業別及指定行業[2]，因此案例中蒐集並利用資料的網友，並不會違反現行的電腦處理個人資料保護法。但依目前官方版的個人資料保護法草案內容，未來自然人將被列為適用對象[3]，且只要以任何方式取得個人資料都屬於個人資料保護法草案定義的蒐集[4]，因此若修正草案通過後，網友在網路上蒐集與使用個人資料的行為，均將有法可管。

另外在行政院衛生署網站上可以查詢醫事人員執業資料[5]，只要輸入姓名，可以查詢專科資格、執業登記場所、執業登記科別及報備支援場所等，若網友在網路上公布波蘭醫學生姓名、任職醫院，因為這些資料是可以在公

[1] 電腦處理個人資料保護法第 3 條第 1 款規定：「個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

[2] 電腦處理個人資料保護法第 3 條第 7 款規定：「非公務機關：指前款以外之左列事業、團體或個人：
(一) 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。
(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。
(三) 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

[3] 個人資料保護法草案第 2 條第 8 款：「非公務機關：指前款以外之自然人、法人或其他團體。」

[4] 個人資料保護法草案第 2 條第 3 款：「蒐集：指以任何方式取得個人資料。」

[5] 行政院衛生署網頁引用之相關法規為醫師法第 10 條第 1 項：「醫師歇業或停業時，應自事實發生之日起三十日內報請原發執業執照機關備查。」、同條第 2 項：「醫師變更執業處所或復業者，準用關於執業之規定。」、第 27 條：「違反第 8 條第 1 項、第 2 項、第 8 條之 2、第 9 條、第 10 條第 1 項或第 2 項規定者，處新臺幣 2 萬元以上 10 萬元以下罰鍰，並令限期改善；屆期未改善者，按次連續處罰。」

開網站上查詢的資料，而且是否具有醫師資格關乎病人權利，具有公益性質，因此公布姓名及執業場所資料尚屬適法，不至於有侵犯隱私權。但是若公布家庭成員、家庭背景等，這些資料往往是個人不欲人知的私領域範圍，而且這些資料也會涉及到其他人的個人資料，公布的話可能會有侵犯隱私權之虞。無遠弗屆的網路雖然有匿名之特性，常常讓人發表不負責的言論，但是若侵害到他人的隱私或名譽，仍然需要承擔法律責任，因此在網路世界仍應謹言慎行。

管理 *Tips*

本案例對網路服務(部落格)，應於使用者註冊或使用期間，適當地告知其所需遵循的法律責任，並可於運作期間，施行定期或不定期抽查，以確認相關內容均不違反法令法規之規範，以確保有盡善良管理者之責任。

對使用者及轉寄信件人員而言應需針對其行為，清楚地辨識其所需遵遁的法令法規，特別針對個人資料的資料保護與隱私權的考量，更應有適當，以避免踰越了法律的規範。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A 15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A 15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：*S980102*】

洩漏考生資料　每筆資料判賠 ***100*** 元懲罰性違約金

【案號：桃園地方法院 *97* 年度訴字第 *1536* 號】

焦點話題

○○公司於 *96* 年 *12* 月與國立桃園高級中學(以下簡稱桃園高中)訂定勞務採購契約，約定由○○公司承攬 *97* 年國中基本學力測驗之電腦報名作業(建立考生基本資料)及各國中集體報名單位考生基本資料等相關電腦作業。○○公司前法定代理人甲○○、現任法定代理人乙○○及實際負責人丙○○等，利用○○公司承攬上開 *97* 年國中基測電腦作業，因而得以知悉、持有 *97* 年國中基測所有考生之個人基本資料及測驗分數資料(含姓名、校代碼、校名、總分、地址、郵區、電話等資料)之電磁紀錄檔案，燒錄成光碟後販售與補教業者，造成合計 *34,975* 名考生資料遭外洩。甲○○經台中地方法院認定構成背信罪及違反電腦處理個人資料保護法，判處有期徒刑 *1* 年 *6* 月、緩刑 *4* 年，並應向公庫支付 *20* 萬元。乙○○及丙○○之犯行經高雄地檢署起訴後，目前由高雄地方法院進行審理中。桃園高中另依勞務採購契約之約定，依○○公司洩漏考生資料人數按每筆 *100* 元計算，向○○公司請求 *3,497,500* 元之懲罰性違約金，經桃園地方法院審理後，判決桃園高中勝訴。

重點摘要

1. 為了確保債務人確實遵守契約的約定事項及義務，可以在契約中約定合理的懲罰性違約金，只要債務人有違反的情況時，債權人即可以向債務人請求賠償，不需要證明實際上是否有受到損害。

2. 政府機關將事務委外處理時，必須特別注意對委外機關或廠商保密義務

的約定，以避免資料外洩時，政府機關要對外負擔損害賠償責任。

法律觀點

桃園地方法院判決○○公司應賠償 *3,497,500* 元之懲罰性違約金，是以雙方勞務採購契約作為依據。依勞務採購契約之約定，考生基本資料、統計結果、閱卷成績等電子資料檔及其他任何形式之相關資料，○○公司均應交給主辦單位「*97* 年國民中學學生基本學力測驗全國試務委員會」(即桃園高中)，不得進行契約之外任何形式的資料運用，如有上開不法情事經檢舉並查明屬實後，每洩漏 *1* 名考生資料應給付 *100* 元之懲罰性違約金。是以甲○○、乙○○及丙○○既然有洩漏考生資料之行為，依約應該給付懲罰性違約金。○○公司雖主張此條懲罰性違約金之金額過高，而請求法院酌減，但法院審酌雙方訂定契約時之經濟狀況，及個人資料保護之必要性，認為 *100* 元之懲罰性違約金合理允當，是以判決桃園高中勝訴。

此判決雖肯定個人資料保護之必要性，但判賠的基礎是依照雙方契約約定，且提起損害賠償者是桃園高中，並非資料遭到外洩的考生，所以不適用電腦處理個人資料保護法(以下簡稱個資法)有關賠償責任的規定。如從考生的立場，本件桃園高中是受教育部委託辦理 *97* 年度國中基測，桃園高中並委託○○公司辦理考生資料電腦處理程序，依個資法第 *5* 條之規定，桃園高中及○○公司均會被視為委託機關之人[1]，因此○○公司將考生資料作為試務範圍以外的使用，考生可能以個資法第 *8* 條第 *1* 項前段[2]之規定，主張受教育部委託的○○公司將個人資料作特定目的以外之使用，而按個資法第 *27* 條[3]之規定向教育部請求損害賠償，損害賠償總額每人每事件以 *2* 萬

[1] 電腦處理個人資料保護法第 5 條：「受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人。」

[2] 電腦處理個人資料保護法第 8 條第 1 項前段:「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。」

[3] 電腦處理個人資料保護法第 27 條第 1 項：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

元以上 *10* 萬元以下計算，最高應負 ***2,000*** 萬元之損害賠償責任，教育部若遭到求償後，則得依契約關係向其委託的桃園高中及○○公司求償。

因此，公務機關事務委外時，在委外廠商有疏失時，是否有將法律要求的賠償責任切實透過契約關係要求委外廠商承擔。同時，必須特別注意委外機關或廠商約定保密義務，並可約定懲罰性違約金，以讓委外機關或廠商能夠確實遵守保密義務，以降低對外負損害賠償責任的風險。

管理 Tips

本案例中已於契約中對委外廠商有安全性之要求，惟應可再考量檢視委外廠商是否有與學校一致之控管水準，另為確保較主動預防此類事件發生，公司應可針對委外廠商重要流程實施定期/不定期之稽核。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.10.2.1 服務交付

應確保包含於第三方服務交付協議內的安全控制措施、服務定義及交付等級已由第三方予以實作、執行及維持。

A.10.2.2 第三方服務的監視與審查

應定期監視與審查由第三方提供的服務、報告及紀錄，並定期執行稽核。

前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。」

類別：資訊保護

【案號：*S980103*】

戶籍謄本列印新制　婚姻紀錄可不曝光

【資料來源：自由時報 *98/08/27*】

焦點話題

過去戶籍謄本記事欄皆會登載結婚、離婚等紀錄，為保護婦女，婦女團體多年來爭取需經當事人同意才能列印記事欄內容，政府自 *98* 年 *8* 月起規定記事欄內資料須經當事人同意始得列印，避免爭議。

對此，曾有婚姻記錄的婦女大多深表歡迎，認為這項新制可保護個人隱私，不只是婦女，男性也可獲相同保障。但也有人認為，此種措施可能讓曾有婚姻紀錄者開始考量要不要欺瞞另一半或準備結婚的對象。

不過，即使有意欺瞞，婚後可能反而過著心驚膽顫的生活，害怕婚姻紀錄曝光，如果不同意記事欄被列印，對方反而懷疑。不過，如果是另一半能夠諒解過去的婚姻紀錄，卻不想被長輩得知，此項新制才有其意義。

雖然政府考量的是婚姻等隱私權，但新制影響所及，還波及一般民眾申請謄本的手續。由於記事欄內資料需獲當事人同意始得列印，要列印全家人的記事欄，便要有全家人的同意書，陳姓民眾日前因而在戶政事務所大發雷霆，指他為赴美子女申請謄本，因應留學所需，依規定必須列印記事欄內容，還要大費周章取得子女的同意書，實在擾民。

重點摘要

1. 婚姻紀錄屬於電腦處理個人資料保護法規範的個人資料，在蒐集及使用資料時，必須遵守相關規定。
2. 公務員在使用民眾個人資料時應該要注意遵守相關規定，避免日後遭到求償。

法律觀點

依電腦處理個人資料保護法第 *3* 條第 *1* 款[1]的定義，婚姻紀錄屬於受到保護的個人資料，因此戶政機關在蒐集或利用個人資料時，應該要遵守電腦處理個人資料保護法的規定。公務機關蒐集、電腦處理或使用個人資料，依照電腦處理個人資料保護法第 *7* 條[2]及第 *8* 條[3]的規定，必須要符合一定的要件。過去民眾依法向戶政機關申請戶籍謄本時，記事欄均會記載婚姻狀況，包括結婚及離婚之紀錄，可能會讓民眾不欲人知的訊息曝光，以進行訴訟為例，法院通常會要求當事人陳報被告的戶籍謄本，並以戶籍謄本上記載的戶籍地址作為送達法院書狀的地址，當事人只要持法院的文件，戶政機關即會准予申請並提供，如此一來，即有可能讓第三人知悉戶籍地址以外的資料，對於民眾的隱私權保障確實有不足之處。因此，此項新制確實是我國保護隱私權的一大進步，值得鼓勵。至於對於民眾產生不便的地方，也應該在便利民眾及保護隱私權間尋求配套措施。

公務機關在依照法令規定執掌的範圍內，雖然可以在特定目的內蒐集電腦處理個人資料，但是在資料的使用及提供上，也應該注意要在必要的範圍

[1] 電腦處理個人資料保護法第 3 條第 1 款：「一、個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

[2] 電腦處理個人資料保護法第 7 條：「公務機關對個人資料之蒐集或電腦處理，非有特定目的，並符合左列情形之一者，不得為之：
一、於法令規定職掌必要範圍內者。
二、經當事人書面同意者。
三、對當事人權益無侵害之虞者。」

[3] 電腦處理個人資料保護法第 8 條：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：
一、法令明文規定者。
二、有正當理由而僅供內部使用者。
三、為維護國家安全者。
四、為增進公共利益者。
五、為免除當事人之生命、身體、自由或財產上之急迫危險者。
六、為防止他人權益之重大危害而有必要者。
七、為學術研究而有必要且無害於當事人之重大利益者。
八、有利於當事人權益者。
九、當事人書面同意者。」

內為之。若違反電腦處理個人資料保護法的規定，公務機關將對受有損害的當事人負損害賠償責任，每人每一事件以新台幣 *2* 萬元以上 *10* 萬元以下計算，最高賠償總額為 *2000* 萬元[4]。若公務員執行職務有故意或重大過失而使公務機關遭求償時，公務機關可依國家賠償法的規定向該公務員求償[5]。因此，公務人員在使用民眾的個人資料時，必須要特別注意，避免因個人故意或重大過失而要負最終的損害賠償責任。

管理 *Tips*

個人隱私的保護為近年來倍受重視，而正在修法中的「個人資料保護法」也增加適用範圍及提高的損害賠償的上限，是以就機關的角度而言，仍應考量相關法律、法令的規範，訂定申請程序、申請要件等，並依此執行業務以避免違反相關法律、法令，另也透過教育訓練及宣導，來使業務執行人員更清楚瞭解所應擔負之法律責任。

另外對民眾也應有適當的宣導及解說，但應避免只單從規定的角度說明，而是要以可能造成民眾個人資料外洩的風險說明，以增加民眾的瞭解及諒解，更適當地於文件上標示警語，提醒民眾的注意。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

[4]電腦處理個人資料保護法第 27 條：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。…」

[5] 國家賠償法第 2 條第 3 項：「前項情形，公務員有故意或重大過失時，賠償義務機關對之有求償權。」

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：*S980104*】

Facebook 流量增加　面臨資料外洩之威脅

【資料來源：台灣醒報 *98/02/03*】

焦點話題

美國知名社交網站 *Facebook* 全球使用人數已超過一億五千萬人，其功能十分多元，除了留言板的功能外，還有相簿、遊戲、隨時動態訊息等，使用者更可以透過群組搜尋，尋找失聯已久的朋友或有共同興趣的網友。然而亦有使用者表示 *Facebook* 提供的訊息過於詳細，有個人資料外洩的危險，而這也是此類社交網站最大的隱憂。

Facebook 因廣告收益日漸減少，故計畫利用其一億五千萬之會員資料建立市場研究資料庫，提供予企業作為市場調查工具，讓跨國公司根據會員的一些個人資料，如單身或已婚，甚至是否為同性戀等，調查市場對新產品的反應。此舉引起使用者質疑隱私權遭受侵害。

對此，警政署表示，除非徵詢使用者同意，否則 *Facebook* 無法使用其個人資料，但如果有民眾因為個人資料洩漏而受害，因 *Facebook* 公司設在國外，故只能將案件轉給當地的警政系統，或者透過我駐外使節處理。

但相關人士透露，除非是牽涉到毒品等國際公罪，或者關係很好的國家，否則當地的警方多半都會因為案件太小，嫌麻煩而拒絕受理。

重點摘要

*1.*個人在註冊網站會員時，應該注意不要提供較為隱密的資料，避免資料外洩或作為其他用途。

*2.*未來個人資料保護法草案通過後，社交網站蒐集會員資料的行為將受到規範，對個人資料可以提供更完善的保護。

法律觀點

基於網際網路的盛行，提供平台讓網友認識朋友或排遣時間的社交網站也越來越熱門。尤其社交網站提供強大的搜尋功能，只要提供的資料越詳細，就越能與其他朋友或同學找到，重拾失聯已久的友情。社交網站雖然可以擴大社交圈，但同時也隱含個人資料外洩或遭利用的風險。

依我國電腦處理個人資料保護法第 3 條第 7 款[1]的規定，此類的社交網站目前並非該法規範的主體，因此，若網友的資料外洩或遭不法利用時，只能在符合民法或刑法之規定時，依該等法律主張權利，並由網友負舉證責任，因此網友主張權利較為困難。

有鑑於此，個人資料保護法草案將擴大適用到所有自然人、法人或團體[2]，惟自然人為單純個人或家庭活動的目的而蒐集、處理或利用個人資料的情況是被排除適用。此外，在個資法草案第 8 條增加告知義務的規定，在進行資料蒐集以前，必須向當事人明確告知蒐集資料的類別、用途及利用狀況等事項[3]。而且對於個人資料的蒐集或處理必須具備特定目的並符合法律規定的情形，除非有例外情況，否則不得將個人資料作為特定目的外的使用。若將個人資料作為行銷用途時，業者必須在首次行銷時免費提供當事人表示拒絕的方式[4]，以尊重當事人的意願。另外，為提昇法益保護的周延，

[1] 電腦處理個人資料保護法第 3 條第 7 款：「非公務機關：指前款以外之左列事業、團體或個人：
(一) 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。
(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。
(三) 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

[2] 個人資料保護法草案第 2 條第 8 款：「非公務機關：指前款以外之自然人、法人或其他團體。」

[3] 個人資料保護法第 8 條第 1 項：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：
一、公務機關或非公務機關名稱。
二、蒐集之目的。
三、個人資料之類別。
四、個人資料利用之期間、地區、對象及方式。
五、當事人依第三條規定得行使之權利及方式。
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。」

[4] 個人資料保護法第 20 條第 2 項：「非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。」、第 3 項：「非公務機關應於首次行銷時，免費提供當事人表示拒絕之方式。」

在中華民國領域外對中華民國人民蒐集、處理或利用個人資料，都適用該法[5]。是以，草案對個人資料的保護將更為完善。

然而，雖然未來外國網站業者對我國國民蒐集或利用資料，會受到個人資料保護法的規範，但是一旦資料外洩或是遭到不法利用的情況下，若該國外網站在台灣沒有辦事處或財產的情況下，受害人恐怕很難請求損害賠償。因此，自我保護的最好方法還是儘量不要提供太多個人資料，以降低風險。

管理 *Tips*

在個人資料保護法修訂後，擴大其適用範圍至所有自然人、法人或團體，是以有從事資料蒐集之自然人、法人或團體應依法令法規之要求，對蒐集所得之個人資料盡良好管理之責，針對個人資料的應用，也均需取得個人之書面同意方可進行使用。

另針對被蒐集資料的個人，則應更加注意資料提供的適當性，在網路上是無國界的，大部分跨國的狀況，並非本國法律所能保護的範圍，是以個人應對此方面的影響，有更完善的認知，並自行多加注意。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

[5] 個人資料保護法草案第 50 條第 2 項：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」

類別：資訊保護

【案號：*S980105*】

採集生物檢體應行告知程序並予以保密

【資料來源：聯合晚報 *98/07/16*】

焦點話題

為有效管理我國生物醫學研究資料庫並維護國民資訊隱私權，「人體生物資料庫管理條例」草案就有關生物檢體的採集，規定應告知實施採集者的身分、所屬機關，採集的目的、使用範圍和期間，採集方法、種類、數量和部位，以及可能的併發症和危險，被選為參與者的原因，還有自生物檢體所得基因資料對參與者及親屬、族群可能造成的影響、預期衍生的商業運用、保障個人隱私的機制等；取得參與者同意後才能進行採集，否則有 *10* 萬元至 *50* 萬元不等的罰鍰。而參與者亦得要求停止提供生物檢體、退出或變更同意範圍，但不得請求資料、資訊的閱覽、製給複製本。

生物資料庫的資料、資訊，僅得用於生物醫學研究之用途，不得用於其他用途，否則亦有 *30* 萬至 *150* 萬元不等的罰鍰責任。

為保護參與者的隱私，設置生物資料庫者就生物檢體和相關資料儲存、運用或揭露時，應以編碼、加密、匿名化、去連結；違者處罰 ***30*** 萬至 ***150*** 萬元不等之罰鍰；相關工作人員，也不得洩露因業務知悉的資料，違者將發生 *3* 萬元至 *15* 萬元不等的罰鍰責任。

重點摘要

*1.*人體生物資料庫管理條例草案為法律允許可以蒐集敏感性資料的法律明文依據。

*2.*人體生物資料庫設置者於採集生物檢體或其他個人資料前應踐行告知程序並取得參與者同意。參與者可以隨時退出參與。

*3.*生物資料庫之運作乃以匿名性連結為基礎，故原則上生物檢體及相關資料、資訊之儲存、運用及揭露，應以無法辨識參與者身分之方式為之。

法律觀點

依個人資料保護法草案第 *6* 條之規定，醫療、基因、性生活、健康檢查及犯罪前科等敏感性資料，除非有該條但書各款所定之例外情形，否則原則上是不能蒐集、處理或利用[1]，人體生物資料庫管理條例草案(以下簡稱生物資料庫草案)即是屬於例外規定。人體生物資料庫草案制定目的是為了促進醫學發展與疾病研究治療，以了解基因與環境諸多因素對於疾病的影響。該草案在第 *3* 條第 *2* 款[2]針對生物資料庫有詳細的定義，其中「自然人資料」包含生物檢體之衍生資料、基因資料、身體檢查資料等[3]，屬於個人資料保護法草案的特別規定，應優先適用。要注意的是，生物資料庫草案對於得設置生物資料庫者之主體有一定的限制，並應向主管機關申請許可[4]，所以不具備該資格而去蒐集生物資料時，仍是違反個人資料保護法草案第 ***6*** 條規定，因此依據同法第 ***40*** 條的規定將有 *2* 年以下有期徒刑的刑事責任，意圖營利者，最高可處 *5* 年以下有期徒刑。

生物資料庫草案第 ***6*** 條規定，採集生物檢體應尊重生命倫理，同時必須將第 *7* 條[5]相關事項告知參與者，並載明於同意書，取得其同意後，才能進行

[1]電腦處理個人資料保護法第 *6* 條：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、法律未明文禁止蒐集、處理或利用，且經當事人書面同意。
三、公務機關執行法定職務或非公務機關履行法定義務所必要。
四、當事人自行公開或其他已合法公開之個人資料。
五、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人。」

[2] 草案第 *3* 條第 *2* 款：「生物資料庫：指為生物醫學研究之目的，以人口群或特定群體為基礎，內容包括參與者之生物檢體、自然人資料及其他有關之資料、資訊，且可自行衍生擴充資料、資訊之範圍，或可取得不同來源之資料、資訊互為連結、比對之資料庫。」

[3] 草案第 *3* 條之立法說明。

[4] 草案第 *4* 條第 *1* 項：「生物資料庫之設置者，以政府機關、醫療或學術機構、研究機構、法人（以下統稱機構）為限，並應向主管機關申請許可。」

[5] 草案第 *7* 條：「前條應告知之事項如下：
一、生物資料庫設置之法令依據及其內容。

採集。另外，賦予參與者可以隨時退出或變更同意使用範圍之機制，且於參與者退出時，原則上其生物檢體及相關資訊、資料應予以銷燬[6]。

此外，生物資料庫設置者應訂定相關安全規範，同時報請主管機關核定並予公開[7]。採集、處理、儲存或使用生物檢體之人員亦負有保密義務[8]。生物資料庫之運作並以匿名性連結為基礎[9]，以保障參與者之資訊隱私權。

管理 *Tips*

本案例中從生物資料庫設置者應先辨識其於業務運作過程(採集、處理、儲存或使用)中所適用之相關法令及法規有那些，特別是針對個人資料保護的

二、實施採集者之身分及其所屬機構。
三、被選為參與者之原因。
四、參與者依本條例所享有之權利及其得享有之直接利益。
五、採集目的及其使用之範圍、使用之期間、採集之方法、種類、數量及採集部位。
六、採集可能發生之併發症及危險。
七、自生物檢體所得之基因資料，對參與者及其親屬或族群可能造成之影響。
八、對參與者可預期產生之合理風險或不便。
九、本條例排除之權利。
十、保障參與者個人隱私及其他權益之機制。
十一、設置者之組織及運作原則。
十二、將來預期連結之參與者健康資料。
十三、生物資料庫之運用原則及程序。
十四、預期衍生之商業運用。
十五、其他與生物資料庫相關之重要事項。」

[6] 草案第 *12* 條：「參與者得要求停止提供生物檢體、退出參與或變更同意使用範圍，設置者不得拒絕。
參與者退出時，設置者應銷毀該參與者已提供之生物檢體及相關資料、資訊；其已提供第三人者，第三人應依照設置者通知予以銷毀。但有下列情形之一者，不在此限：
一、經參與者書面同意繼續使用之部分。
二、已去連結之部分。
三、為查核必要而須保留之同意書等文件，經倫理委員會審查同意者。」

[7] 草案第 *10* 條：「設置者應訂定生物檢體及相關資料、資訊之安全規範，並公開之。前項規範應報主管機關核定。」

[8] 草案第 *13* 條：「採集、處理、儲存或使用生物檢體之人員，不得洩漏因業務而知悉或持有參與者之秘密或其他個人資料、資訊。」

[9] 草案第 *16* 條：「設置者就生物檢體及相關資料、資訊為儲存、運用、揭露時，應以編碼、加密、匿名化、去連結或其他無法辨識參與者身分之方式為之。
設置者就參與者姓名、國民身分證統一編號及出生年月日等可辨識個人之資料，應予加密並單獨管理；於有與其生物檢體及相關資料、資訊相互連結運用之必要時，應建立審核與控管程序，並應於為必要之運用後立即回復原狀。
設置者為不同來源之資料、資訊互為連結、比對時，應依第一項規定為之，並應於連結、比對後，立即回復原狀。
參與者同意書、終止參與研究聲明書等無法與可辨識參與者之資料分離之文件，不適用前三項規定。但設置者應採取其他必要之保密措施。」

部分，並據此設計所需的控管措施，並於法律所許可的範圍下使用資料。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：*S980106*】

機場電腦故障　境管門戶洞開

【資料來源：自由時報 *98/01/07*】

焦點話題

桃園機場的電腦系統停擺，移民署出入境資訊系統大當機，經過 *36* 小時後終於修復。移民署表示當機原因在於磁碟陣列機損壞，造成資料庫系統發生嚴重故障，使入出境查驗電腦無法運作，不涉及人為疏失。而因移民署與合作廠商在契約中有約定，若相關系統故障時必須在 *6* 小時內修復，此次當機長達 *36* 小時，已屬違約，因此將依據合約向合作廠商求償。

對於移民署將求償一事，合作廠商 *A* 公司表示將與移民署溝通，因 *A* 公司甫拿到移民署電腦系統維護標案，尚未正式與移民署簽約，亦未點收機器或完成交接，因此將電腦故障超時維修之責任完全轉由 *A* 公司承擔並不公平。

然而，除了超時維修責任歸屬之疑義外，電腦系統故障還衍生出境管門戶洞開之問題，行政院已要求內政部等單位儘速做好危機處理及安全補漏等措施。

重點摘要

*1.*若將系統營運維護委託外部廠商營運時，應特別注意時間的銜接性，以免發生資訊安全漏洞。

*2.*委外廠商合約到期時，應確實辦理交接，以利後續系統之運作及維護。

法律觀點

本件主要問題在於事件發生時，*A* 公司才剛標得護照查驗系統的維護案，尚未與原來維護廠商辦理交接，導致 *A* 公司因不了解系統架構及概況，無法

在最短的時間內修復系統，相關的個人入出境管理資料僅能暫時以人工查驗，入出境管理發生漏洞。

有關個人出入境資料，應為電腦處理個人資料保護法(以下簡稱個資法)第 *3* 條第 *7* 款所稱之「社會活動」[1]，屬於個人資料，因此受到該法保護。移民署乃是基於法定職務蒐集個人出入境資料，依個資法第 *13* 條第 *1* 項[2]規定，公務機關應維護個人資料的正確性，且依 *17* 條之規定，公務機關如果保有個人資料檔案，便應該指定專人辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏[3]，因此若本件因為磁碟陣列機損害造成個人出入境資料滅失，或因人工查驗作業導致個人出入境資料不正確，均屬於違反個資法的規定，若因此造成民眾損害，應負損害賠償責任。再者，依照個資法第 *5* 條規定[4]，*A* 公司在個資法適用範圍內將被視為委託機關之人，因此在個資法適用範圍內，委託機關亦須對委外廠商疏失行為負責。

本件案例突顯了系統維護時間銜接及工作交接的重要性，因此公務機關將系統維護案委外時，應注意時間的銜接性並在契約明定交接義務，避免因為後承接廠商對系統的不熟悉，造成處理時間的延宕。另外，也應該在契約裡明確要求委外廠商遵守個資法的相關規定，以拘束委外廠商的行為，並降低損害。

管理 Tips

本案例中就移民署的角度，針對護照查驗業務與系統仍應負責最終的權責，合約罰款只是事後的控制，並無法有效降低事件所招致的衝擊，是就

[1] 電腦處理個人資料保護法第 *3* 條第 *1* 款：「本法用詞定義如左：
一、個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

[2]電腦處理個人資料保護法第 13 條：「公務機關應維護個人資料之正確，並應依職權或當事人之請求適時更正或補充之。」

[3] 電腦處理個人資料保護法第 17 條：「公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」

[4] 個資法第 *5* 條：「受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人。」

移民署的角度在系統相關事物有重大變更時，應進行適當評估，並依評估結果進行預防及避免重大事故的發生，是以在本案例，移民署應於更換委外維護時，評估所帶來的風險，並同時審視於原來營運持續計畫內容的合宜，如：通訊聯絡資料、負責人員及考量人員執行能力等因素後，修改相關文件，以確保在重大災害時組織的因應能力。

另本案例有部分原因是由於新承接之廠商進行維護時，不熟悉系統而導致系統嚴重毀損，是以組織因針對重要系統/設備訂定維護規則，並依維護規則對系統/設備執行維護。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.9.2.4 設備維護

應正確地維護設備，以確保其持續的可用性與完整性。

A.10.2.1 服務交付

應確保包含於第三方服務交付協議內的安全控制措施、服務定義及交付等級已由第三方予以實作、執行及維持。

A.10.2.2 第三方服務的監視與審查

應定期監視與審查由第三方提供的服務、報告及紀錄，並定期執行稽核。

A.10.2.3 第三方服務變更的管理

所提供服務的變更，包含維持與改進現有的資訊安全政策、程序及控制措施均應加以管理，並考量所涉及之營運系統與過程的重要性以及風險的重新評鑑。

A.10.3.1 容量管理

應監視、調諧(*tune*)各項資源的使用，並對未來容量要求預作規劃，以確保所要求的系統效能。

A.14.1.2 營運持續與風險評鑑

應識別能導致營運過程中斷的事件，與此等中斷事件的機率及衝擊，以及其後果對資訊安全的影響。

A.14.1.5 營運持續計畫的測試、維護及重新評鑑

營運持續計畫應定期測試與更新，以確保維持最新且有效。

類別：資訊保護

【案號：*S980107*】

防個資外洩　別填身分證字號

【資料來源：自由時報 *98/09/10*】

焦點話題

消基會調查發現，多家餐飲店、大賣場及通信販賣業者在消費滿意度問卷、抽獎券或販賣型錄內容報告上，會要求民眾提供過多個人資料，包括身分證字號及地址，甚至與業者服務品質改善無關的學歷、服務機構等資料亦一併要求民眾提供，故消基會呼籲民眾要提高警覺，拒絕填寫過多的個人資料，例如身分證字號，以免個人資料外洩而受害。

消基會並表示，業者如果因為疏失讓個人資料外流致當事人受損害時，業者要負損害賠償責任，同時提醒業者要在有效監督下確認資料銷毀。

針對個人隱私資料外洩的疑慮，目前已有大賣場表示辦抽獎或請消費者填問卷，只要求消費者留電話和姓名或會員卡號，不會要求消費者留身分證字號；而亦有大型超市重新設計對獎存根聯，讓民眾自行上網核對號碼。

重點摘要

*1.*蒐集或利用個人資料應在特定目的之必要範圍內進行，與特定目的無關的個人資料應不得蒐集。

*2.*消費者在填寫資料時，應注意不要提供過多的資料，避免隱私權

受到侵害。

法律觀點

現今企業為進行行銷，會透過很多方式及管道蒐集個人資料，包括填寫問卷或抽獎卷，無形中讓個人資料外洩，被作為其他行銷目的的用途，甚至讓詐騙集團利用，導致許多無辜民眾受騙，因此個人資料的保護日益重要且應該重視。

經濟部以 *93* 年 *12* 月 *1* 日經商字第 *09302195240* 號函[1]指定資本額新台幣 *1000* 萬元以上之股份有限公司，採會員制為行銷方式之百貨公司業及零售式量販業，自 *94* 年 *2* 月 *1* 日起適用電腦處理個人資料保護法(以下簡稱個資法)，因此若符合上述函示所列要件的百貨及零售業者，在蒐集個人資料時即應該遵守相關規定。依個資法第 *6* 條的規定，個人資料的蒐集或利用，應尊重當事人權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，換言之，蒐集個人資料的類別應該限於特定目的必要範圍。

目前個資法僅規範 *8* 大行業及經主管機關指定適用的行業[2]，其他非公務機關或自然人，均非規範主體，對於個人資料的保護有所不足，因此個人資料保護法草案(以下簡稱個資法草案)，擴大規範主體，所以非公務機關及自然人均受到規範。依個資法草案第 *5* 條的規定，增加必須與蒐集目的具有正當合理關聯的規定。依個資法草案第 *19* 條的規定，餐飲店、大賣場、通信販賣業者等非公務機關

[1]經商字第 09302195240 號：「公告指定登記資本額為新臺幣一千萬元 (含) 以上之股份有限公司之組織型態，且有採會員制為行銷方式之百貨公司業及零售式量販業為電腦處理個人資料保護法第 3 條第 7 款第 3 目之非公務機關，並自中華民國 94 年 2 月 1 日起適用電腦處理個人資料保護法。」

[2] 電腦處理個人資料保護法第 3 條第 7 款：「非公務機關：指前款以外之左列事業、團體或個人：
(一) 徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人。
(二) 醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業。
(三) 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人。」

固然可以在一般民眾消費後，因締結契約關係或經過民眾同意而蒐集、處理民眾的個人資料，作為業者服務品質改善的參考依據或者是作為抽獎、贈獎活動聯繫上的方便[3]。但是，這些業者蒐集民眾的個人資料時，所蒐集的資料與蒐集的目的之間必須具有正當合理的關聯性，不能夠超過該目的必要範圍。換言之，如果業者蒐集民眾個人資料的目的是為了改善服務品質，那業者只能夠蒐集與「改善服務品質」有關的個人資料，身分證字號即屬於不相關的個人資料。

為了保障民眾的個人資料隱私權，除了有關單位應督促業者守法以及業者應該自律外，民眾也必須自己提高警覺，以免不小心就洩漏了過多個人資料。

管理 *Tips*

在此案例中對業者而言，在蒐集個人相關資料前應先行辨識其所適用的法令法規，並依此評估當蒐集後組織所可能面臨的風險，據此評估蒐集相關的個人資料是否妥適且必要，以降低保存個人資料所延伸的風險。

而對民眾而言，也應如法律觀點內所提應自行提高警覺，避免提 供過多的個人資料。

相關標準

[3] 草案第 19 條：「非公務機關對個人資料之蒐集或處理，應有特定目的，並符合下列情形之一者：
一、法律明文規定。
二、與當事人有契約或類似契約之關係。
三、當事人自行公開或其他已合法公開之個人資料。
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過處理後或依其揭露方式無從識別特定當事人。
五、經當事人書面同意。」

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：*S980108*】

勾結員警盜賣個資　檢方起訴不法集團

【資料來源：中央社 *98/12/9*】

焦點話題

熊姓女子所組成的個資盜賣集團，涉嫌自民國 *95* 年起從縣市警察局等單位購買個資，再販賣給徵信業者。台北地檢署偵查終結，將熊世芬等 8 人依違反個資法等罪起訴。

檢方指出，熊女自 *95* 年起開始販賣個資，每筆消息收受新台幣 *1500* 元至 *2* 萬 *8000* 元不等的費用，每月收入達 *10* 萬至 *15* 萬元。*96* 年 *9* 月間，熊女委託曾某利用分局內的「內政部警政署戶役政查詢系統」，查詢 *5* 名民眾的個資後，販賣給徵信業者。

檢方表示，熊女又在 *97* 年 *4* 月間與謝某談妥調取個資價碼，謝某隨後假藉辦案名義，向電信業者調閱 *3* 支行動電話的通聯紀錄。

重點摘要

1. 不法蒐集或利用個人資料，可處 *2* 年以下有期徒刑、拘役或科或併科新臺幣 *4* 萬元以下罰金，公務員利用職務上機會，將加重其刑至 *1/2*。

2. 對於員警基於職務能夠查詢非辦案目的的戶政資料及調閱通聯紀錄，應確實執行控管導正程序，以免違法並導致機關負有國家賠償責任。

法律觀點

戶籍資料的建立，主要是為了管理國家人口，依電腦處理個人資料保護法第 *8* 條[1]之規定，公務機關對個人資料之利用，應於法令職掌必要範圍內為

[1] 電腦處理個人資料保護法第 8 條：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。但有左列情形之一者，得為特定目的外之利用：
一、法令明文規定者。

之，並與蒐集之特定目的相符。且須有法律所列情況，始能為目的外使用。警員基於辦案需求，可以透過「內政部警政署戶役政查詢系統」查詢民眾戶籍資料，應屬於增進公共利益，可作為特定目的外的利用。

然而這也意味著民眾的戶籍資料可能會在不知不覺中即被查詢、甚至外洩。對於案例中警員洩漏個人資料及熊女不法蒐集並利用個人資料的情況，依照電腦處理個人資料保護法 *33* 條[2]規定，可以處 *2* 年以下有期徒刑、拘役或科或併科新臺幣 *4* 萬元以下罰金。另警員因係利用職務上的方法，加重其刑至 *1/2*[3]。此外，民眾若因此受有損害時，也可以依照電腦處理個人資料保護法第 *27* 條[4]規定，請求國家賠償。

基於維護社會秩序及公共利益，開放警員於辦案之必要範圍內，開放查詢民眾資料，惟應限制警員可以查詢資料之類別，並建立控款機制，如此一來，可以維護社會秩序，並增加人民對政府的信賴感。

管理 Tips

現行政府機關存放了許多個人隱私資料，如戶政的戶籍資料、財稅的稅務

二、有正當理由而僅供內部使用者。
三、為維護國家安全者。
四、為增進公共利益者。
五、為免除當事人之生命、身體、自由或財產上之急迫危險者。
六、為防止他人權益之重大危害而有必要者。
七、為學術研究而有必要且無害於當事人之重大利益者。
八、有利於當事人權益者。
九、當事人書面同意者。」

[2] 電腦處理個人資料保護法第 33 條：「意圖營利違反第 7 條、第 8 條、第 18 條、第 19 條第 1 項、第 2 項、第 23 條之規定或依第 24 條所發布之限制命令，致生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 4 萬元以下罰金。」

[3] 電腦處理個人資料保護法第 35 條：「公務員假借職務上之權力、機會或方法，犯前 2 條之罪者，加重其刑至 1/2。」

[4] 電腦處理個人資料保護法第 27 條：「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。
第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」

資料、健保的就醫紀錄與投保資料等，對民眾而言，均為高度敏感的資料，是以資料的保護非常重要，而且此案例中所提及的檢警調機構為查案之用可透過系統查詢相關資料，但由於所查詢資料均為高度敏感，是以均應有適當的存取紀錄，並遂筆覆核其存取之合理性，以確保不會違反民眾的權益及法令的要求，並可針對處理相關業務的同仁，進行教育訓練讓相關人員瞭解相關法令上的責任及可能造成的影響。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

二、國家機密保護法

類別：資訊保護

【案號：*S980201*】

拍攝資電中心　陸客誤入不起訴

【資料來源：聯合報 *98/07/10*】

焦點話題

台灣高檢署偵辦大陸觀光客馬 OO 闖入「資電作戰指揮部」刺探軍機案，認為馬 OO 並非故意入侵軍事處所，而且沒有刺探或收集國防機密的意圖，作成不起訴處分。

馬 OO 被控闖入國防部資電作戰指揮部拍了三張照片，疑是共諜，遭憲兵隊逮捕送辦。

檢方調查，國防部人才招募中心與資電作戰指揮部的營區操場僅有一門之隔，馬 OO 未被告知不得進入資電中心，現場也沒有任何禁止進入、禁止拍照等標誌，研判馬 OO 並非有意侵入資電中心拍照。

馬 OO 在營區拍攝的照片雖然遭軍方人員刪除，但調查局回復後檢視，發現這三張照片分別是營區內軍車停放、營區內人員身著運動服跑步及國軍國家責任榮譽標語的照片，都和軍事機密無關。

重點摘要

1. 刑法的處罰必須出自行為人的故意行為，除非刑法有特別規定才處罰過失犯。
2. 刺探或收集之資料，必須與國防或軍事機密有關，才會構成刺探或收集國防機密罪。

法律觀點

本案例馬 OO 的行為可能違反刑法第 *112* 條[5]不法侵入或留滯軍用處所罪與第 *111* 條[6]刺探蒐集國防機密罪。在刑法第 *112* 條的部分，必須是基於刺探刑法第 *109* 條第 *1* 項之「中華民國國防應秘密之文書、圖畫、消息或物品」之意圖，不法進入或留滯軍用處所。至於刑法第 *111* 條刺探蒐集國防機密罪，在客觀方面，必須刺探蒐集的對象屬於刑法第 *109* 條第 *1* 項之國防機密。主觀方面，必須行為人具備故意[7]，若行為人本身不是故意的，雖然可能有過失，但因該條沒有處罰過失犯的特別規定，所以不會構成刑事犯罪。本案例因為國軍人才招募中心與資電中心僅有一門之隔，馬 OO 拍照當時該門並未關閉，且門上或旁邊沒有任何禁止進入之標誌，也沒有人員在現場告知不得進入，因此並非故意進入資電中心營區，且軍方人員制止馬 OO 後即將他帶到國防部人才招募中心，因此馬 OO 未留滯在現場。而馬 OO 拍攝的照片是軍車停放、營區人員身著運動服跑步及國軍國家責任榮譽標語的照片，並不涉及中華民國國防應秘密的文書、圖畫、消息或物品，因此給予馬 OO 不起訴處分。

國防機密或軍事機密屬於國家機密的一種，國家機密保護法對於國家機密之保護有詳細的規定。國家機密保護法所稱的國家機密，必須經過國家機密保護法規定核定機密等級[8]。依其機密程度可以分成絕對機密、極機密及機密等級，且在核定國家機密等級時，必須一併核定保密期限或解除之條件，並明確標示。其後，國家機密的收發、傳遞、使用、持有、保管、複製及移交，應依其等級分別管制，並有一定程序的要求[9]。在此案例裡沒有

[5] 刑法第 112 條：「意圖刺探或收集第一百零九條第一項之文書、圖畫、消息或物品，未受允准而入要塞、軍港、軍艦及其他軍用處所建築物，或留滯其內者，處一年以下有期徒刑。」

[6] 刑法第 111 條第 1 項：「刺探或收集第一百零九條第一項之文書、圖畫、消息或物品者，處五年以下有期徒刑。」

[7] 刑法第 12 條規定：「行為非出於故意或過失者，不罰。
過失行為之處罰，以有特別規定者，為限。」

[8] 國家機密保護法第 2 條：「本法所稱國家機密，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者。」

[9] 參考國家機密保護法施行細則第 17 條以下之規定。

提到所涉相關事物是否涉及國家機密，但若有涉及國家機密，相關權責人員即應依法核定機密等級，以受到國家機密法之保護。另外，若屬於軍事重地，非得任意進入時，即應在近入口處明確標示禁止進入的警語，並派駐人員在現場駐守，以確保有心人士進入刺探及蒐集。應注意的是，如果主管機關已經明示禁止出入場所，擅自出入不聽勸阻者，除有觸犯前述法律責任之虞外，依據社會秩序維護法之規定，最高可處 *6,000* 元以下罰緩[10]。

管理 *Tips*

本案例中的大陸觀光客馬 OO 所違反之情事，主要應為不知情是以未追究任何後續責任，因未知規定而導致違反規定實應施以加強之宣導與教育訓練，惟若以此案例而言，實無法有合適的對象範圍去實行宣導或教育訓練，但以「資電作戰指揮部」就管理角度仍可再一步考量對所管轄涉及敏感之區域，清楚鑑識及劃分為安全區域，並設立清楚的標示警語，避免他人違反規定，但警語的設置仍應適當考量是否會因此反而落入此地無銀三百兩之窘境。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.9.1.1 實體安全周界

應使用安全周界(諸如牆、卡控入口閘門或人員駐守的接待櫃檯等屏障) ，以保護含有訊及資訊處理設施的區域。

A.9.1.2 實體進入控制措施

安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出。

[10] 社會秩序維護法第 71 條：「於主管機關明示禁止出入之處所，擅行出入不聽勸阻者，處新台幣六千元以下罰鍰。」

三、營業秘密法

類別：資訊保護

【案號：*S980301*】

離職員工借密碼　遠銀安泰打官司

【資料來源：聯合報 *98/02/20*】

焦點話題

遠東和安泰兩家民營銀行，因為員工涉嫌竊取商業機密鬧上法院。金融界人士透露，一名遠東銀行離職員工跳槽到安泰銀行後，跟以前在遠銀熟識的同事借用帳號及個人密碼，在安泰銀行上網進入遠銀內部網路，被遠銀資訊部門發現。遠銀為避免內部作業機密外流，具狀控告安泰銀行竊取商業機密。遠東及安泰銀行都已經開除借密碼、用密碼的員工。

安泰銀行表示此事純屬員工個人行為，安泰高層並沒有做任何指示，因此與安泰銀行沒有任何關係，且安泰銀行在第一時間已開除該名員工，安泰沒有疏失。但遠銀認為應該由法院判定。

金融圈人士指出，銀行人員流動率很高，員工將自己使用者帳號及密碼交由其他人使用的情況可能防不勝防，各銀行都要提高警覺。法院判決結果，可能會成為往後銀行處理類似案件的參考。

重點摘要

1. 受僱人執行職務時不法侵害他人權利時，僱用人除非能夠證明其選任受僱人及監督其職務之執行已經盡相當之注意義務，或縱加以相當之注意仍不免發生損害，否則僱用人必須負連帶賠償責任，不可以其屬員工個人行為加以卸責。

2. 加強員工對資訊安全的認識及約束，並教育員工帳號密碼應該嚴加保管

及保密。

法律觀點

現在多數公司除了公開網站供一般民眾閱覽外，常常會另外建置公司內部網站，網站內容常常是不欲外人知的公司機密資訊及管理制度作業，目的是讓員工可以進入系統查詢公司內部資料或客戶資料，並可以在線上填寫工作日誌及填寫假單等事宜，如此一來，可以達到公司內部資源共享之目的，且對於公司內部程序可以省去傳遞之不便。

但是許多公司網站的管理，都如同本案例之情況，是由員工輸入帳號及密碼來進入系統，因此若員工未保管好帳號密碼或洩漏帳號密碼給第三人之情況下，第三人將很容易可以進入公司內部網站，並獲悉或取得公司機密資料。本案例中該名安泰銀行行員將會觸犯刑法第 358 條[1]入侵電腦或相關設備罪，會有 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金之刑責之虞。至於提供帳號密碼的員工，可能構成共犯外，亦有可能涉嫌違反刑法第 317 條[2]洩露業務上知悉工商秘密罪。所謂「工商祕密」，係指工業上或商業上之秘密事實、事項、物品或資料，而非可舉以告人者而言，重在經濟效益保護[3]，通常員工進入公司內部網站之帳號密碼，應該屬於商業上不可洩露給第三人的秘密資料，因此該名員工恐另有 1 年以下有期徒刑、拘役或 1 千元以下罰金刑責之虞。

至於安泰銀行雖然表示該行為純屬員工個人行為，安泰高層並沒有做任何的指示，但是依照民法第 188 條第 1 項[4]之規定，受僱人在執行職務時，不

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[2] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」

[3] 臺灣高等法院 78 年度上易字第 2046 號判決參照。

[4] 民法第 188 條第 1 項：「受僱人因執行職務，不法侵害他人之權利者，由僱用人與行為人連帶負損害賠償責任。但選任受僱人及監督其職務之執行，已盡相當之注意或縱加以相當之注意而仍不免發生損害者，僱用人不負賠償責任。」

法侵害他人權利時，僱用人必須負連帶賠償責任，因此只要受僱人的行為在客觀上足以認為是執行職務時，僱用人原則上即必須負連帶賠償責任。本案例安泰銀行員工在安泰銀行上網進入遠東銀行內部網路，就法律觀點來說是有可能遭認定是屬於執行職務之行為，若安泰銀行擬免責，必須要證明該行於選任受僱人及監督職務執行，已盡相當之注意，或縱加以相當之注意而仍不免發生損害。因此，安泰銀行表示純屬員工個人行為、高層沒有指示，最終還是要由法院認定是否具有免除安泰銀行連帶賠償責任之事實存在。

管理 *Tips*

本案例可從遠銀及安泰的角度分開檢視其管理面可再參酌之處。

對遠東銀行方面應再檢視以下幾方面之管理現況是否有可再加強之處：

1. 「機密性協議」的簽定：對現行員工是否有明確限定並明確告知其保密之責任與義務，而對離職員工部分是否有考量協議簽定之有效期限，針對組織之重要及敏感資訊，可考量於協議上清楚註明離職後仍具有保密的責任，並不只限於在職期間。

2. 通行碼(密碼)保管之責任：現行員工應對其通行碼有妥善保管責任，組織可再藉內部宣導或教育訓練之機會加強說明員工其保管的責任及洩漏所導致的風險。

3. 網路區隔：針對重要系統或僅供公司內部使用之系統，應有適當之網路區隔，避免其他人可從外部隨意連線以提高其安全性。

而從安泰銀行方面則可再檢視其「機密性協議」的簽定：可針對員工到職時所簽定之機密性協議加註相關規範，並於內部宣導及教育訓練時加強宣導。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A5.2.2 訓練、認知及能力

組織應確保在 ISMS 中界定之被指定責任的所有人員，有能力執行並瞭解其所被賦與之資安責任。

A 8.1.3 聘僱條款與條件

身為契約義務的一方，員工、承包商及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A 11.3.1 通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

A 11.4.5 網路區隔

應將資訊服務、使用者及資訊系統各群組使用的網路加以區隔。

類別：資訊保護

【案號：*S980302*】

離職員工偷機密　與老東家削價競爭

【資料來源：中央社 *98/08/03*】

焦點話題

台北市警局偵破離職員工盜取老東家商業機密，並開設業務性質相同公司，以惡意削價手法與原公司競爭的案件。警方將蔡姓、陳姓嫌疑人依妨害秘密等罪移送法辦。

警方表示，*7*月初接獲某清潔公司報案指稱，公司內部相關機密檔案遭日前離職的蔡姓、陳姓兩人複製竊取，於是展開調查。

警方發現，兩名嫌疑人不顧離職時已簽訂「員工保密保證書」等文件，另開設相同業務性質的公司，並以竊自老東家的客戶基本資料及承包金額底價文件，用更低價格惡意競標原公司客戶，導致原公司損失約 *350* 萬元。

警方查獲蔡姓、陳姓兩人後，將全案依妨害秘密、妨害電腦使用、違反著作權等罪，移送士林地檢署偵辦。

重點摘要

1. 並非所有公司資料都可以構成營業秘密，必須符合一定的法律要件。

2. 若員工有簽署保密契約書，就應該對保密契約內容約定的事項負保密義務，而不以構成營業秘密為限。

法律觀點

一家公司的成功經營，往往會有該公司特有的技術與經驗，就是所謂的「*know-how*」。這些技術與經驗大部分是公司長久研發或投入市場後，傳承下來所累積的寶貴智識，具有一定的經濟價值，一旦被不法人士竊取並投入市場競爭後，將對該公司造成極大的損害，因此為了維護競爭秩序，且

鼓勵公司能夠致力於研發及經營，因此我國在民國(下同)*85* 年 *1* 月 *17* 日公布施行營業秘密法。

依照營業秘密法第 *2* 條[1]的規定，所謂營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，且必須具備祕密性、具有實際或潛在的經濟價值且已採取合理之保密措施等三個要件。換言之，並非所有公司的資料都是營業秘密，必須是不為一般涉及該資訊的人員能夠普遍了解或者獲得，且必須具備經濟價值，同時也要採取合理的保密措施，才能夠受到營業秘密法的保護。由於營業秘密法保護的客體有要件的限制，為了保護公司商業機密，避免員工不知道該資訊是公司機密，或在資料外洩後爭執該資料不屬於營業秘密，因此公司通常會要求員工簽署保密切結書，並在保密切結書中約定應保密的範圍，讓員工知道其應該負保密義務的範圍，並在營業秘密法保護之外，賦予員工契約上義務，確保公司資料不被外洩。

著作權法保護之著作必須具備原創性，只要完成著作時，即受到著作權法的保護，包括著作人格權[2]及著作財產權[3]。依著作權法第 *11* 條[4]之規定，受雇人於職務上完成的著作，若契約未特別約定之情況下，以受雇人為著作人，但著作財產權由雇用人享有。因此，受雇人在未經公司授權之情況下，重製或散布著作物，即有侵害公司著作權之虞。

---

[1] 營業秘密法第 2 條：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：
一、非一般涉及該類資訊之人所知者。
二、因其秘密性而具有實際或潛在之經濟價值者。
三、所有人已採取合理之保密措施者。」

[2] 包括公開發表權、姓名表示權及禁止不當修改權。

[3] 包括重製權、公開口述權、公開播送權、公開上映權、公開演出權、公開傳輸、公開展示權、改作權、散布權等。

[4] 著作權法第 11 條：「受雇人於職務上完成之著作，以該受雇人為著作人。但契約約定以雇用人為著作人者，從其約定。
依前項規定，以受雇人為著作人者，其著作財產權歸雇用人享有。但契約約定其著作財產權歸受雇人享有者，從其約定。
前二項所稱受雇人，包括公務員。」

本案例蔡姓及陳姓員工的法律責任，違反刑法第 *317* 條[5]洩漏業務上知悉工商秘密罪，依刑法第 *318* 之 *2* 條[6]規定，利用電腦設備犯第 *317* 條時，得加重其刑至二分之一。而該兩名員工無故自公司電腦取得資料，也構成刑法第 *359* 條無故取得電磁紀錄罪[7]。此外，若該二名員工自電腦重製之資料為著作權保護之著作時，同時違反著作權法第 *91* 條第 *1* 項[8]之規定。

民事責任部份，依營業秘密法第 *13* 條[9]之規定，被害人可以選擇依民法第 *216* 條[10]之規定請求賠償，也可以選擇請求侵害人所得之利益。而且如果是故意侵害的情況，法院也可以依照被害人的請求，酌定侵害額以上的賠償，但不能超過侵害額的三倍。

公司內部機密資料屬於公司寶貴資產，除了法律賦予之相關保護規定外，公司更應建立一套完整的營業秘密管理制度，對資料採取適合的保護措施，以維護公司的權利。

管理 Tips

從本案例中來看蔡姓、陳姓嫌疑人，前公司特別要求員工於離職前再簽署「員工保密保證書」，所以 *2* 人應是故意的行為，組織如要預防此類之行為，

---

[5] 刑法第 317 條：「依法令或契約有守因業務知悉或持有工商秘密之義務，而無故洩漏之者，處一年以下有期徒刑、拘役或一千元以下罰金。」

[6] 刑法第 318 之 2 條：「利用電腦或其相關設備犯第三百十六條至第三百十八條之罪者，加重其刑至二分之一。」

[7] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

[8] 著作權法第 91 條第 1 項：「擅自以重製之方法侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣七十五萬元以下罰金。」

[9] 營業秘密法第 13 條：「依前條請求損害賠償時，被害人得依左列各款規定擇一請求：
一、依民法第二百十六條之規定請求。但被害人不能證明其損害時，得以其使用時依通常情形可得預期之利益，減除被侵害後使用同一營業秘密所得利益之差額，為其所受損害。
二、請求侵害人因侵害行為所得之利益。但侵害人不能證明其成本或必要費用時，以其侵害行為所得之全部收入，為其所得利益。
依前項規定，侵害行為如屬故意，法院得因被害人之請求，依侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之三倍。」

[10] 民法第 216 條：「損害賠償，除法律另有規定或契約另有訂定外，應以填補債權人所受損害及所失利益為限。
依通常情形，或依已定之計劃、設備或其他特別情事，可得預期之利益，視為所失利益。」

可從資料之存取與保全方面著眼思考：

如員工為離職前取得資料，一般存取控管可從以下 *3* 個層面為思考起點：

1. 資料庫或系統管理帳號的存取控管：此部份應從組織存取權限授與的合理性做為考量起點，應僅授與員工執行業務最小權限，並有適當的監控機制，至少做到有第 2 人可以監控其存取行為是否合理，惟此部份之控管與造成之影響(傷害)較大，組織應審慎考量或儘量避免開放此類存取。

2. 使用應用程式存取：除合適之權限授與外，也應避免員工一次可取得大量資料著手，例如使用 *Web* 查詢畫面，使用者僅可 *1* 次存取單筆資料，使組織所遭遇之風險降低。

3. 注意可攜式儲存媒體的使用管控，儘量避免使用可攜式儲存媒體存取敏感資料，如此可使大量資料外洩的機率降低。

另如為員工於離職後取得的話，則應加強落實人員離職時存取權限的移除，以避免此類狀況的發生。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.8.3.3 存取權限的移除

所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

A.10.7.1 可移除式媒體的管理

應有適當的程序以管理可移除式媒體。

A11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A11.6.1 資訊存取限制

應根據所界定的存取控制政策，限制使用者與支援人員對資訊與應用系統功能之存取。

四、刑法

類別：資訊保護

【案號：*S980401*】

怕被打壓開會錄音，被檢方起訴

【資料來源：中央社 *98/06/16*】

焦點話題

國防部軍備局專員 *OOO*，本身兼任該局考績委員會委員，因害怕遭長官打壓，在軍備局召開有關他的考績委員會時，攜帶錄音器材至現場，並在會議要求迴避時，將錄音器材放置在會場內，竊錄其他委員的評論。

OOO 表示他雖然有將錄音機放置在會場內，但是當天並未宣讀保密規定，況且他先前遭長官打壓，當天為了保障自己權益，才會進行錄音。

檢方認為考績會並非國家機密保護法所稱涉及國家機密會議，無須宣讀保密規定，且 *OOO* 為考績委員會委員因深知規定，且軍備局已依考績法規定給予陳述意見之機會，因此以妨害秘密罪起訴。

重點摘要

1. 在沒有正當理由之情況下，不可以使用設備竊錄他人非公開之談話。

2. 法規規定之應秘密事項均應予以保密，不會因為是否有宣讀保密規定而有差別。

3. 對考績事項之內容應嚴守秘密。

4. 現役軍人犯法時，應先依陸海空軍刑法進行軍法審判，若陸海空軍刑法無特別規定時，由普通法院依刑法審判。

法律觀點

現代科技日新月異，電子產品設備推陳出新，雖然給人類的生活帶來極大

的便利性，但同時也讓窺探他人隱私活動越來越容易，基於現今社會對於個人隱私權之保護日益重視，因此刑法第 *315* 之 *1* 條[1]特別就無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者，設有處罰之規定。

依照陸海空軍軍官士官考績條例第 *10* 條[2]之規定，辦理陸海空軍現役中將以下軍官、士官之考績時，對於考績事項應該要嚴守秘密，因此在召開考績委員會時，應屬於非公開之活動及言論。至於考績委員會之會議規則或許有保密規定宣讀之程序，然而此屬於程序規定，若會議之本質屬於法律規定應秘密之事項，不會因為是否有宣讀保密規則而影響其為應秘密事項之本質，因此該名專員在沒有正當理由之情況下，用錄音器材竊錄考績委員會之開會過程，構成妨害秘密，但因為陸海空軍刑法沒有妨害秘密罪章之規定，因此依刑法第 *315* 之 *1* 條第 *2* 款規定來論罪。

管理 *Tips*

本案例可從以下 *2* 方面再行確認國防部軍備局控管狀況：

*1.*宜再確認是否有明確界定成員依其所負責業務應負有的資訊安全責任，應考量以下項目：

- 宜識別與明確界定與每一特定系統相關的資產及安全過程。

- 宜明確定義授權層級，並予以文件化。

2. 在完成界定資訊安全責任後，組織可藉由「保密契約」的簽定來使負責業務同仁清楚知道所應負的資安責任，再於日常期間加強進行資訊安全教育訓練來提昇同仁的資訊安全認知，以避免其違反相關法令法規或組

[1] 刑法第 315 之 1 條：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：
一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。
二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[2] 陸海空軍軍官士官考績條例第 10 條：「考績官及辦理考績人員，對考績事項應嚴守秘密，並不得徇私失實或遺漏錯誤；違者，應按情節輕重予以懲處。」

織的規範。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A 6.1.3 資訊安全責任的配置

應明確界定所有資訊安全責任。

A 8.1.3 聘僱條款與條件

身為契約義務的一方，員工、承包商及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。

類別：資訊保護

【案號：*S980402*】

戶籍資料不慎外洩　戶政事務所課員遭起訴

【資料來源：中央社 *97/08/18*】

焦點話題

一名戶政事務所課員，因提供另一名同名同姓者個人資料給申請者，造成他人陷入訴訟，因而遭到檢察官依洩露秘密罪嫌聲請法院簡易判決處刑。

一家法律事務所人員因訴訟需要，向戶政事務所申請訴訟相關人員的戶籍資料，受理這起申請案的陳姓戶政課員，一時不察，而提供另一名同名同姓者的戶籍資料，造成這名無辜者陷入不必要的訴訟事件，憤而向警方報案追究刑事責任。

面對檢警的訊問，這名戶政課員坦承提供戶籍資料，但辯稱是申請人只提供姓名，並非故意提供他人戶籍資料。

但地檢署檢察官調查後發現，律師事務所人員申請時已附上相關的地址，並非只有姓名，所以認定戶政課員涉嫌洩露國防以外秘密，向法院聲請予以簡易判刑。但念其經驗不足，且一時失慮，所以也建議法院從輕量刑，並給予緩刑機會。

重點摘要

1. 公務員因為過失而洩漏國防以外機密時，構成洩露國防以外機密罪。
2. 公務員基於職務提供資料時，必須仔細核對申請文件上所載事項，以確認提供資料對象者的身分。

法律觀點

在法院進行訴訟時，法院通常會要求提起訴訟的原告，提供被告的最新戶籍謄本，以作為送達法院文書的地址。但因戶籍資料屬於個人資料，應該

屬於國防以外的機密，因此若不是本人、受託人或利害關係人[1]，戶政事務所即不應該提供相關資料。因此在申請戶籍謄本時，應該檢附相關資料，例如法院要求提供戶籍謄本之通知函，以釋明利害關係。相關規定只有例示利害關係之情況，如何確認利害關係並未進一步規定需要提供的證明文件，因此戶政人員在受理戶籍謄本申請時，必須依照申請人提供證明文件，以判斷是否符合法令規範。

在本案例裡面，法律事務所因訴訟需要，向戶政事務所請求抄錄戶籍謄本，屬於利害關係人委託申請之代理人，因此戶政機關應依法提供，並無疑義。然而，在本案例裡，戶政人員不慎提供另一位同名同姓的地址，因為戶籍資料上載有姓名、身分證字號，出生年月日、戶籍地址等足資辨識個人之資料，屬電腦處理個人資料保護法之範疇，公務人員不得為特定目的外之使用[2]，且此等資料必須透過戶政系統電腦始得查詢，係屬於國防以外之機密，且戶政人員在受理本案戶籍謄本申請時，法律事務所有提供被申請人的地址，戶政人員未比對申請資料之記載，而提供錯誤的資料，在職務上顯有疏失，刑法第 *132* 條[3]第 *2* 項針對洩漏國防以外機密罪的過失犯設有處罰規定，因此縱使該名戶政人員不是故意洩漏他人資料，也難免被追究相關刑事責任。此外，公務機關因洩露個人資料，亦應依電腦處理個人資料

[1] 以臺北市各區戶政事務所受理閱覽抄錄及交付戶籍登記資料作業要點之規定為例，第 4 條第 2 項即規定：「第一項第二款所稱之利害關係人，指與當事人具有下列各款情形之一者：
（一）契約未履行或債務未清償。
（二）同為公司行號之股東或合夥人，且為執行職務所必要。
（三）訴訟繫屬中之兩造當事人。
（四）當事人之配偶、直系血親、直系姻親或旁系三親等內之血親。
（五）戶長與戶內人口。
（六）其他確有法律上權利義務得喪變更之關係。」

[2] 電腦處理個人資料保護法第 8 條：「公務機關對個人資料之利用，應於法令職掌必要範圍內為之，並與蒐集之特定目的相符。…」

[3] 刑法第 132 條第 1 項及第 2 項：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。
因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。」

保護法第 *27* 條[4]之規定負損害賠償責任。

公務人員職權範圍內常常會接觸到機密資料，且因應政府資訊公開法之實施，政府資訊是以公開為原則，因此在依法提供資料給申請人時，必須注意提供資料的正確性，且要特別注意提供的資料是否屬於依法不得提供或限制提供之機密資料，以免觸法。

管理 *Tips*

於本案例中戶政事務所課員非惡意的洩漏個人資料而導致受害人遭受無故的困擾，此狀況就組織管理面可從以下 *2* 個層次來做確認，可先行檢視組織於相關規範是否完善，如申請時是否進一步需要個人身分證字號來確認身分，才可較增加其可信性及確認之有效性，如組織規範尚屬不足，則需針對資料的存取及處理訂定完善的程序，如已有相關規定，但因人員未落實而導致事件的發生，則需考量進一步的加強教育訓練及宣導，並加強確認教育訓練的成效，如考試等。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A5.2.2 訓練、認知及能力

組織應確保在 *ISMS* 中界定之被指定責任的所有人員，有能力執行並瞭解其所被賦與之資安責任。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職

[4] 電腦處理個人資料保護法第 27 條:「公務機關違反本法規定，致當事人權益受損害者，應負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。
被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
前二項損害賠償總額，以每人每一事件新臺幣二萬元以上十萬元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
基於同一原因事實應對當事人負損害賠償責任者，其合計最高總額以新臺幣二千萬元為限。
第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。」

務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.1.1 文件化作業程序

操作程序應加以文件化、維持，並讓有需要的所有使用者均可隨時取得。

A 15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊保護

【案號：*S980403*】

製作山寨版人事局網頁　以偽造公文書送法辦

【資料來源：聯合報 *98/08/09*】

焦點話題

網路出現山寨版的行政院人事行政局網頁，搶先發布莫拉克颱風停班停課不實訊息；刑事局查出，○○公司廖姓、林姓程式設計師涉案，兩人到案認錯坦承「玩笑開過頭了！」。

刑事局接獲人事行政局報案。警方循線查出○○公司林姓程式設計師將假網頁的網址，上傳到 *PTT* 電子布告欄，在中華電信網頁空間存放假網頁檔案的申請人，則是○○公司廖姓員工，鎖定兩人涉嫌重大。

廖姓及林姓員工到案後，廖姓員工坦承跟同事開玩笑，下載人事局停班停課表格，胡亂改寫一通後上傳中華電信網頁空間，將連結網址 *MSN* 給同事；林姓員工也認為好玩，把網址貼到 *PTT* 布告欄，沒想到一發不可收拾。

廖姓及林姓員工因冒用政府機關名義製作不實網頁，提供不實訊息，依刑法偽造公文書罪嫌函送法辦。

重點摘要

1. 網頁的資訊可以表示一定的用意，屬於刑法上的準文書，必須有權限製作的人才可製作並發布，否則會構成偽造文書罪。

2. 網路雖然具備匿名性的特質，但網路上的行為仍必須遵守法律規定，若有違法行為，即使純粹只是開玩笑，還是難逃相關刑事責任的追究。

法律觀點

現今社會共同生活及經濟活動中，各式各樣的文書扮演重要的角色，文書的內容可以表達文書製作者的意思，既可以證明權利，也可以作為締約當

事人約定一定權利義務的證明，因此文書可以確保社會經濟活動的安全性及可靠性，因此有保護文書真實性的必要。

本案例中廖姓及林姓員工可能會涉嫌刑法第 *211* 條偽造公文書罪[1]及第 *216* 條[2]行使偽造文書罪。所謂公文書，指的是公務員職務上製作的文書[3]。而為了因應電腦資訊及網際網路時代，透過機器或電腦處理後顯示的聲音、影像或符號，足以表達一定的意思，亦為刑法規範的文書[4]，一般稱作「準文書」。行政院人事行政局負責行政院所屬機關之人事行政，並負責公告公務機關假期及颱風天上班上課情況，因此人事行政局公布停班停課的網頁，屬於公務員職務上所製作的準文書，必須有製作權限的人事行政局或其所屬公務員，才能夠發布停班停課的相關訊息。

廖姓員工冒用人事行政局名義，將自行製作的網頁上傳至免費網頁空間，讓不特定人都可能點選該網頁，因而誤信偽造網頁上的停課停班訊息。林姓員工將錯誤網頁所在的網址發布到電子布告欄，屬於行使偽造公文書的行為，兩人可能面臨 *1* 年以上 *7* 年以下有期徒刑之刑責。另外廖姓員工下載停班停課表的行為也可能會構成刑法第 *359* 條破壞電磁紀錄罪[5]。

廖姓及林姓員工本意均只是出於開玩笑的心態，但是他們將不實的訊息公布至網路上，可能會使不知情的民眾誤信，因此仍應依相關規定負刑事責任。網際網路的社會雖然具備匿名性的特性，但行為仍會受到法律的規範，是以仍應該要謹言慎行，避免誤觸法網。

管理 Tips

於本案例中廖姓、林姓程式設計師因開玩笑之心態假冒人事行政局之網

[1] 刑法第 211 條：「偽造、變造公文書，足以生損害於公眾或他人者，處 1 年以上 7 年以下有期徒刑。」

[2] 刑法第 216 條：「行使第 210 條至第 215 條之文書者，依偽造、變造文書或登載不實事項或使登載不實事項之規定處斷。」

[3] 刑法第 10 條第 3 項：「稱公文書者，謂公務員職務上製作之文書。」

[4] 刑法第 220 條第 2 項：「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。」

[5] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

頁，似乎不知其後果之嚴重性(違反「偽造公文書」之法令)，是以針對此案例而言應考量加強對人員法律相關知識之宣導與教育訓練，並確認教育訓練的成效，如考試等。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

類別：資訊保護

【案號：*S980404*】

台哥大跨年當機　工程師搞鬼

【資料來源：聯合報 *98/09/01*】

焦點話題

台灣大哥大行動電話用戶在跨年夜時大當機，檢調查出是○○公司前工程師陳姓員工，涉嫌以女友名義登入台灣大資料庫並刪除資料造成大當機，檢方依妨害電腦使用罪嫌將陳姓員工起訴。

陳姓員工原任職於台灣大哥大維護商○○公司，負責台灣大哥大的 *SRRi* 主機（門號可攜認證系統）及 *TA* 主機（客戶話務計費系統）維護，除了熟知兩主機的操作與相關指令外，還知悉登入的帳號密碼。陳姓員工遭公司解雇心生不滿，刻意挑選話務量最大的跨年夜，拿女友申辦的台灣大哥大手機連線到台灣大哥大兩大主機，將主機內的可攜號碼資料與連線登入紀錄全數刪除，並重新啟動系統，卻因資料全部刪光，導致無法重新開機，停擺時間從當晚 *11* 時 *25* 分直到隔天凌晨 *4* 時許才恢復。

台灣大哥大當機造成數萬用戶受害，無法撥打行動電話，簡訊、語音信箱等也無法使用，損失約 *1500* 萬元。陳員否認是遭開除而挾怨報復，僅說會這麼做是因為「好玩」。

重點摘要

1. 沒有正當理由，不可以使用他人的帳號密碼登入電腦系統，或是破壞他人電腦或相關設備的電磁紀錄，否則會構成妨害電腦使用相關刑事責任。
2. 對於員工因職務上所知悉的營業秘密或技術，公司可以透過契約的約定，約束員工在職及離職後，必須負保密義務且不得為職務以外之利用，以保護公司本身及客戶的權益。

3. 針對公司委託廠商進行相關服務時，公司應注意在契約上約定委託廠商及其所屬員工負保密義務，並不得作委託範圍以外的使用，以保護公司自身權益。

法律觀點

本案例中陳姓員工涉及的是刑法有關妨害電腦使用罪章之相關規定。陳姓員工涉及犯罪的行為包括使用女友手機連線並登入至台灣大哥大主機、將主機內的可攜號碼資料與連線登入紀錄全數刪除。依照刑法第 358 條[1]之規定，無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，構成無故侵入電腦及相關設備罪，可處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。至於陳姓員工將主機內可攜號碼資料與連線登入紀錄全數刪除之行為，造成台灣大哥大主機大當機之情況，屬於刑法第 359 條[2]規定「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者」之情況，可處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。而就民事責任而言，台灣大哥大可以就其因此所受損害請求賠償。至於○○公司之責任，因為本件陳姓員工已自○○公司離職，因此除非契約有特別約定外，否則○○公司就陳姓員工的侵權行為可以不負連帶賠償責任。

在分工合作之社會裡，公司常常必須將部分事物委託給外包廠商處理，因此公司相關營業秘密、設備及技術，不可避免的會被委外廠商的員工接觸並知悉，因此主機或設備遭到入侵或破壞之風險必然會提高。因此，為降低主機被入侵竊取資料或破壞之風險，公司應該與委外廠商確實約定保密義務，並將委外廠商所有可能會接觸到資料、設備及技術之人作為規範客體。另外，委外廠商對於會接觸到公司及客戶機密資料之員工，不論是在

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處 3 年以下有期徒刑、拘役或科或併科 10 萬元以下罰金。」

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。」

職員工或已離職員工，都仍然應該約定其應負的保密義務，已確實遵守與客戶間的保密約定，而降低被求償之責任。同時，為避免不易舉證員工違反資料使用或保密義務時造成公司的損害數額，亦得考慮於相關契約內約定懲罰性違約金，減少舉證上的困難。但若違約金約定若過高時，法院可以依實際情況裁量酌減[3]。

管理 *Tips*

本案例係因委外廠商之離職員工使用已知之帳號密碼從遠端對系統進行破壞，就管理面而言可從以下 3 個面向加強：

1. 案例中已於契約中對委外廠商有安全性之要求，惟應可再考量委外廠商之內部控制措施是否足夠，如：其員工如能存取本公司之系統或資訊，則應和本公司內部控管程序有一致之控管水準，另為確保能主動預防此類事件發生，公司應針對委外廠商重要流程實施定期/不定期之稽核。

2. 員工(包含員工、承包者及第三方使用者)離職之時應符合公司之離職規定，應於離職之時立即刪除或停用員工帳號，以避免類似事件發生。

3. 該員工使用手機遠端存取系統導致系統中斷；遠端存取較一般存取會少了實體門禁、網路、網域等存取限制，是以組織應特別針對遠端存取進行加強的控管措施,如:雙重身份認證、一次性密碼*(One Time Password; OTP)*等，以避免此類風險的發生。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.8.3.1 終止責任

執行聘僱終止或變更的責任應明確的界定與指派。

A.8.3.3 存取權限的移除

[3] 民法第 252 條：「約定之違約金額過高者，法院得減至相當之數額。」

所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

A.10.2.1 服務交付

應確保包含於第三方服務交付協議內的安全控制措施、服務定義及交付等級已由第三方予以實作、執行及維持。

A.10.2.2 第三方服務的監視與審查

應定期監視與審查由第三方提供的服務、報告及紀錄，並定期執行稽核。

A.11.4.2 外部連線的使用者鑑別

應使用適當的鑑別方法，以控制遠端使用者的存取。

類別：資訊保護

【案號：*S980405*】

竊飛彈資料　技術員涉貪污

【資料來源：聯合報 *98/10/01*】

焦點話題

某研究機構技術員 A○○退休前，抱了一堆飛彈零件規格、技術手冊等資料回家意圖欲販售圖利，被依外患罪查辦，事後雖鑑定這些資料非機密，反觸犯刑責更重的貪汙罪，基隆地檢署偵結起訴。

起訴書指出，A*92* 年間從服務 *27* 年的某研究機構退休前，分批將許多補給手冊影印後攜出，並藏在家中伺機出售。國安局與海調處在調查軍品商人時，發現有商人○○曾在 *95* 年間向他購買資料光碟。

檢調在 A 家搜索查扣到 *4* 大箱資料，並發現他逐筆為這些資料，訂出數千元到十多萬元不等價格。國防部鑑定後，認為這些包括某研究機構電話號碼簿、天弓及天劍等飛彈的相關資料內容老舊，不具機密性，因未構成洩漏交付國防秘密罪而未起訴，但他涉侵占公物罪刑責反而更重。

檢察官認為 A 侵占的公有物品「秤斤量兩也不值幾塊錢」，卻涉及本刑為無期徒刑或十年以上重刑，比公務員洩漏交付國防秘密罪處的刑度更重，雖將他起訴，但代他向法院請求從輕量刑。

重點摘要

*1.*洩漏交付國防機密罪的成立，必須符合遭洩漏的客體具備機密性的要件。

*2.*公務員若將職務所保管的公物據為己有，將依貪污治罪條例追訴刑責。

*3.*公務機關對於機密資料應該嚴格管控，且人員離職或調動時，並應確實辦理交接，避免國家機密或公務機密遭到外洩。

法律觀點

本案例檢察官本來是以刑法第 *109* 條[1]洩漏交付國防機密罪進行偵辦，但該條規範的客體必須為國防機密，A 自某研究機構攜回的飛彈零件規格及技術手冊，因為資料老舊，所以被認定並非國家機密，

但 A 為公務員，依貪污治罪條例第 *2* 條的規定，公務員只要觸犯該法的規定，即依照該法處罰，因此貪污治罪條例適用所有的公務員。又依照貪污治罪條例第 *4* 條第 *1* 款[2]之規定，竊取或侵占公用或公有器材、財物者，處無期徒刑或十年以上有期徒刑。A 涉嫌將飛彈零件規格、技術手冊帶回家，涉嫌竊取侵占公用財物，即構成前述的侵占公物罪。

此案例特別的地方在於，A 侵占的資料價值不高，惟所涉刑度最輕刑度竟為 *10* 年以上有期徒刑，連檢察官都認為顯不相當而請求法院從輕量刑。因此，公務員對於公共財物的保管必須小心謹慎，以避免涉嫌公物侵占的重罪。同時，公務機關也應該要隨時注意機密資料的管控，人員離職或調動時，也要確實辦理交接，避免機密資料被外洩而損害公共利益。

管理 *Tips*

此案例我們將對組織面及對 A○○ *2* 方面探討，首先對組織而言，在此案例中針對重要資訊(手冊)的保存應再衡量控管之完整，包含依法令識別所管理之相關機敏性文件及文件取得、重製、使用等作為，應有更嚴格之做法，如僅能在特定地點閱讀，不可影印等，另承載機敏性資訊之媒體(紙本文件、可攜式儲存媒體或光碟等)的攜出入應有適當之控管；最後對於人員離調職時，更應進行完整之交接，將使用者所保管之重要資訊(含紙本或電磁紀錄)/財物(資訊設備)確實辦理交接，而此部分則應從各人員手上所持有之資訊/財物清冊的完整性開始管理，以利於後續工作交接時，能確認交接項

[1] 刑法第 109 條第 1 項：「洩漏或交付關於中華民國國防應秘密之文書、圖畫、消息或物品者，處一年以上七年以下有期徒刑。」

[2] 貪污治罪條例第 4 條第 1 款：「有下列行為之一者，處無期徒刑或十年以上有期徒刑，得併科新台幣一億元以下罰金：一、竊取或侵占公用或公有器材、財物者。....」

目之完整性。

另對 A○○則應可在其行為所涉及之法律權責，再加強說明及宣導，使人員均可瞭解其行為的影響，以期能發揮嚇阻之效用。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.8.3.2 資產的歸還

所有員工、承包者及第三方使用者在其聘僱、契約或協議終止時，應歸還其擁有的所有組織資產。

A.9.2.7 財產的攜出

未經事前授權，設備、資訊或軟體不應帶出場外。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

類別：資訊保護

【案號：*S980406*】

購物網站標錯價　疑遭駭客入侵

【資料來源：中央社 *98/09/28*】

焦點話題

○○家具連鎖店的購物網站傳出標錯價事件，千元禮券錯標成 *0* 元，估計 *10* 小時內湧進的訂單共計 *64* 億筆，涉及禮券總金額達新台幣 *6.4* 兆元。

消保官表示，○○公司代表至消保會說明，並澄清此次事件並非是標錯價格，因為網站上根本沒有賣禮券，禮券是消費者以 *20* 元積 *1* 點，累積 *3000* 點就贈送 *1* 張 *1000* 元的禮券，因為是贈送品，在內部電腦資料上價格是「*0* 元」。

○○公司說明，屬於內部電腦資料的禮券並沒有貼在公開的網站上，但有駭客入侵轉貼在公開的網站上，並破解公司每 *1* 種商品限制售出 *50* 件以內的程式，導致後來有 *4000* 多筆訂單，合計消費額達到 *6.4* 兆元，

○○公司強調第一時間已關閉主機，消保會也對○○公司提出 *3* 項要求，首先是關閉主機；其次是在 *30* 日提出遭駭客入侵的證明及有適當的解決方案；顧客的資料除提供警方偵查外，不做其它使用。

重點摘要

1. 網路購物網站應該加強網站資訊安全的維持，避免因遭駭客入侵或系統出問題，導致衍生消費爭議。

2. 若網路購物網站標錯價時，在證明對於標價錯誤沒有過失時，可以撤銷標錯的價格。

法律觀點

網路購物是現在時興的消費方式，消費者可以在任何地方透過網路完成交

易，為民眾帶來很大的方便，資策會產業情報研究所預估，*2009* 年台灣網路購物市場規模將達到新台幣 *3,116* 億元，較去年成長 *30.4%*[1]，可見網路購物市場發展的潛力不容小覷。

本案例○○公司表示禮券是點數兌換贈品，因此在公司內部網站裡標示為 *0* 元，但有駭客入侵而將此標價貼在公開網頁上。駭客入侵○○公司內部網站的行為，會構成刑法第 *358* 條無故入侵他人電腦罪[2]。至於駭客將○○公司於內部電腦將禮券標示為 *0* 元的資訊變更成在網站上的公開資訊，也會構成刑法第 *359* 條無故變更他人電腦電磁紀錄罪[3]。此外，○○公司因此侵入行為所造成的損害，也可以對駭客請求民事的損害賠償。至於更改數量的部份，若並非以破解電腦保護措施方式進行，而是程式本身的漏洞時，應不會構成刑事犯罪，若是以破解電腦保護措施之方式，則應視具體行為方式判斷其相關刑責。

至於○○公司對於消費者的責任，除非○○公司有預先保留決定接單與否的權利，否則依照民法第 *154* 條第 *2* 項規定，貨物標定價格陳列時，視為要約[4]，因此網友進行下單時，雙方即對買賣契約產生合意，雙方都必須受到契約的拘束。但因為禮券標示的價格並不是○○公司的意思，依照民法第 *88* 條[5]的規定，○○公司對於標價錯誤沒有過失時，可以撤銷標錯的價格。因此，○○公司恐怕必須證明對於網站的維護沒有過失，才能夠以駭客入侵為由，撤銷標錯的價格，但依民法第 *91* 條[6]的規定，對於信賴標錯價格的

[1] 資料來源 http://mic.iii.org.tw/intelligence/pressroom/pop_pressfull.asp?sno=173&type1=2。
[2] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」
[3] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」
[4] 民法第 154 條第 2 項：「貨物標定賣價陳列者，視為要約。但價目表之寄送，不視為要約。」
[5] 民法第 88 條第 1 項：「意思表示之內容有錯誤，或表意人若知其事情即不為意思表示者，表意人得將其意思表示撤銷之。但以其錯誤或不知事情，非由表意人自己之過失者為限。」
[6] 民法第 91 條：「依第八十八條及第八十九條之規定撤銷意思表示時，表意人對於信其意思表示為有效而受損害之相對人或第三人，應負賠償責任。但其撤銷之原因，受害人明知或可得而知者，不在此限。」

消費者因此遭受的損害，仍有民事損害賠償責任。然而，對於明明知道是網站標錯價格卻下單的網友，○○公司並無民事賠償責任。

因此，網路購物業者應該要謹慎維護網站資訊安全，避免遭駭客入侵，且在產品資訊公開於網站前，也要再三確認標示的資訊是否正確，否則一旦標示價格展示產品後，即會構成民法上的要約，網友下單後，契約即為成立有效，負有履約責任。更重要的是，此種事件可能會影響到公司的商譽，造成的損害恐怕不是金錢可以客觀衡量的。

管理 *Tips*

就本案例而言，最主要之關鍵點在於標錯價格是否為○○公司之過失，是以對○○公司來說，可從為○○公司過失及非○○公司過失 *2* 方面分別探討其管理之需求，如為○○公司過失，則應再從網站資訊的管理再行加強，包含線上資料更新的適當核可、資料更新後的確認等環節，另外也可考量依商業邏輯合理性設計檢查機制，對於不合乎常理的下單進行限制或特別審核，例如採購數量過大或是短時間密集重複下單等行為，以確認其控管之完整性，如為非○○公司過失，則應從網站的防護機制再行加強，包含：網站伺服主機之防護機制(防毒、防駭-修補程式更新、弱點掃瞄)、網路的防護機制(防火牆、入侵偵測/防禦系統的設置)及應用程式的防護(避免後門程式- *Code review*)等機制。

另外公司也應考量在相關的控管程序、授權機制及防護機制是否有留存適當的控管紀錄，足資可在法律上證明已盡良善管理之責任，避免相關法律權責。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.10.4.1 對抗惡意碼的控制措施

應實作防範惡意碼的偵測、預防及復原控制措施以及適切的使用者認

知程序。

A.10.6.1 網路控制措施

網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與應用程式的安全，包括輸送中資訊。

A.10.9.1 電子商務

應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改。

A.10.9.2 線上交易

應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(*mis-routing*)、未經授權的訊息修改，未經授權的揭露，未經授權的訊息複製或重演。

A.10.9.3 公眾可用的資訊

應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改。

A.10.10.1 稽核存錄

稽核日誌係記錄使用者活動、異常及資訊安全事件，宜產生與保留一段議定的期間，以協助未來的調查與存取控制監視。

A.10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.12.6.1 技術脆弱性控制

應取得關於使用中資訊系統之技術脆弱性的及時資訊、評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。

A.13.2.3 證據的收集

在涉及法律行動(民事或刑事)的資訊安全事故後，對人員或組織的跟催措施，應收集、保存及呈現證據，以符合在相關審判時提出證據的規則。

A.15.1.3 組織紀錄的保護

應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損及偽造。

五、醫師法

類別：資訊保護

【案號：*S980501*】

洩露病人減重　醫師被罰

【資料來源：聯合報 *98/12/8*】

焦點話題

減重名醫林○○接受媒體訪問時，透露病人孫○○向他求診減重過程，還出示孫的個人資料，台北市衛生局調查後寄發公文，將他依違反「醫師法」處罰鍰 *10* 萬元，並移由醫師懲戒委員會處理。

衛生局調查發現，林○○於訪談中提及孫到診所求診，減重 *10* 公斤，腰圍也縮小，並提及以針灸、埋線等方式治療及看診頻率，涉及病人隱私；此外還出示孫的資料供媒體拍攝，違反醫師法第 *23* 條，醫師對於因業務知悉或持有他人病情或健康資訊，不得無故洩漏。衛生局表示，被裁罰人若不服，可於文到後 *30* 日內提出訴願。

林○○在受訪後隔天即鞠躬道歉，但由於違背醫學倫理，衛生局將全案再移付醫師懲戒委員會，預計 *1* 個月內會做出決議，可能懲戒包括警告、一定時數繼續教育或臨床進修、停業 *1* 個月以上 *1* 年以下、廢止執業執照、廢止醫師證書等。

重點摘要

1. 醫師對於病人的病情及健康資訊應該負保密義務，否則除會受到懲戒外，還可能面臨刑事追訴及民事損害賠償責任。

2. 醫師保密範圍不限於病人病情及健康資訊，只要是業務所知悉的秘密，即應負保密義務。

法律觀點

醫師任務是照顧病人的生命及健康為使命，因此醫師除須具備高度專業以外，更應遵守醫師倫理規範，以維護醫師執業尊嚴及專業形象。病人病情及就醫資訊屬於高度隱私資料，一般人大多不願意外洩，是醫師法規定，除非醫師受到有關機構之詢問或委託鑑定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩漏[1]，違反者，處新臺幣 *2* 萬元以上 *10* 萬元以下罰鍰[2]。另外醫師倫理第 *11* 條規定：「醫師應尊重病人隱私權，除法律另有規定外，醫師不無故洩漏因業務而知悉之病人秘密。」因此，保密義務亦屬醫師倫理規範，屬於醫師法第 *25* 條[3]移送懲戒事由，最嚴重會受到廢止醫師證書的懲處[4]。

刑事責任部分，林○○雖違反電腦處理個人資料保護法第 *23* 條規定，但其非出於意圖營利的意圖，所以不符電腦處理個人資料保護法第 *33* 條刑罰要件。惟依照刑法第 *316* 條規定，醫師無故洩漏因業務知悉或持有之他人秘密者，處 *1* 年以下有期徒刑、拘役或 *5* 萬元以下罰金，且資料遭到外洩的病人，可以依照電腦處理個人資料保護法第 *27* 條及第 *28* 條規定，請求 *2* 萬元至 *10* 萬元之損害賠償，若能證明金額高於前述金額時，則不在此限。

---

[1] 醫師法第 22 條：「醫師受有關機關詢問或委託鑑定時，不得為虛偽之陳述或報告。」、同法第 23 條：「醫師除依前條規定外，對於因業務知悉或持有他人病情或健康資訊，不得無故洩露。」

[2] 醫師法第 29 條：「違反第 11 條至第 14 條、第 16 條、第 17 條或第 19 條至第 24 條規定者，處新臺幣 2 萬元以上 10 萬元以下罰鍰。」

[3] 醫師法第 25 條：「醫師有下列情事之一者，由醫師公會或主管機關移付懲戒：
一、業務上重大或重複發生過失行為。
二、利用業務機會之犯罪行為，經判刑確定。
三、非屬醫療必要之過度用藥或治療行為。
四、執行業務違背醫學倫理。
五、前 4 款及第 28 條之 4 各款以外之業務上不正當行為。」

[4] 醫師法第 25-1 條第 1 項：「 醫師懲戒之方式如下：
一、警告。
二、命接受額外之一定時數繼續教育或臨床進修。
三、限制執業範圍或停業一個月以上一年以下。
四、廢止執業執照。
五、廢止醫師證書。」

應注意的是，上述有關醫師所應遵守之保密義務，應不僅限於病人病情及健康資訊，只要是因為業務所知悉的秘密，都在保密範圍之列，因此醫師除應妥善保管病歷及就醫紀錄等記載病人隱私資料之文件外，更應謹言慎行，小心秘密從口而出。

管理 *Tips*

電腦處理個人資料保護法現正於立法院進行修法，修法之後將適用於所有保有個人資料的組織，是以就管理面而言，組織應更嚴謹地去處理所有有關個人資料的保存，從個人資料的辨識、資料的保存、使用的授權等，均需有更嚴格的控管，也應針對所有辨識出的個人資料外洩及可能造成的影響，對有可能接觸到病歷的相關人員進行宣導，以確保對組織不會有違法的疑慮。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.7.2.1 分類指導綱要

資訊依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保

護與隱私。

貳、資訊公開（*Disclosure*）

一、政府資訊公開法

類別：資訊公開

【案號：*D980101*】

法官評鑑委員會會議紀錄非屬應公開之政府資訊

【案號：最高行政法院 *98* 年度判字第 *404* 號】

焦點話題

甲因與乙間給付工資小額訴訟事件，不服台灣高等法院 94 年度再抗字第 *37* 號民事裁定，請求台灣高等法院將承審庭長及法官共 *6* 名，移送法官評鑑委員會評鑑。台灣高等法院認為甲聲請評鑑事件，非屬法官評鑑辦法第 *2* 條所定嚴重違反辦案程序事項的案件，且依法官評鑑辦法第 *3* 條規定，個人並無聲請評鑑之權利，亦不得聲請覆審，因此否准其請求。甲遂以政府資訊公開法第 *7* 條第 *1* 項第 *10* 款及行政程序法第 *46* 條規定，請求台灣高等法院提供法官評鑑委員會審查小組審議 *6* 名庭長和法官之會議紀錄，台灣高等法院否准其請求。甲不服，提起訴願，訴願遭駁回後，遂提起行政訴訟，台北高等行政法院及最高行政法院審理後，均認為本件不符合政府資訊公開法第 *7* 條第 *1* 項第 *10* 款及行政程序法第 *46* 條之規定，而駁回甲請求。

重點摘要

1. 政府資訊公開法規定應主動公開之合議制機關會議紀錄，是指依法獨立行使職權的成員具有常設性質的決策性組織，因此臨時任務性編組之會議紀錄，即不是政府應主動公開之資訊。

2. 行政決定前的擬稿及其他準備作業文件，不在應公開的範圍內。

法律觀點

基於政府資訊透明化的要求，除了行政程序法第 *46* 條第 *1* 項 [1]之規定外，

[1] 行政程序法第 46 條第 1 項：「當事人或利害關係人得向行政機關申請閱覽、抄寫、複印或攝影有關資料或

94 年 *12* 月 *28* 日公布的政府資訊公開法，對於政府資訊公開有詳細的規定。依照政府資訊公開法的規定，政府資訊依性質可以分成政府應主動公開、應限制公開或不予公開的資訊及依申請公開等三類，因此，除了法律有特別規定外，民眾可以依照政府資訊公開法的規定請求閱覽抄錄相關資料。有了政府資訊公開法之實施，可以建立政府資訊公開制度，便利人民共享與共同利用政府資訊，並保障人民知的權利，更可達到人民監督政府的效果，促進人民參與公共事物，以增進民主社會之發展與進步。

但最高行政法院之所以駁回甲的請求，主要是認為政府資訊公開法第 *7* 條第 *1* 項第 *10* 款[2]之「合議制機關會議紀錄」，是指「依法獨立行使職權之成員組成具有常設性質之決策機關」[3]，而甲所稱之「法官評鑑委員會審查小組」，並非法律或法官評鑑辦法或法官個案評鑑作業注意事項規定之法定組織，而是機關內部對於是否進行法官評鑑程序之臨時任務編組，自非政府資訊公開法第 7 條第 *1* 項第 *10* 款所稱之合議制機關。

此外，法官評鑑委員會審查小組的審查過程、紀錄及意見等相關文件，僅是向所屬法院建議是否有進行法官評鑑必要的內部其他作業準備文件，依照行政程序法第 *46* 條第 *2* 項[4]第 *1* 款之規定，也不在公開範圍之內，因此駁回甲的請求。

管理 Tips

在政府資訊公開法的規定，政府機關單位應可全面重新檢視組織內的資訊，適當的標註其公開狀況，如主動公開、公開但需經申請、不可公開等，更進一步針對不可公開之部分，清楚敘明相關理由供民眾參考。

卷宗。但以主張或維護其法律上利益有必要者為限。」

[2] 政府資訊公開法第 7 條第 1 項第 10 款：「下列政府資訊，除依第十八條規定限制公開或不予提供者外，應主動公開：…. 十、合議制機關之會議紀錄。」

[3] 政府資訊公開法第 7 條第 3 項：「第一項第十款所稱合議制機關之會議紀錄，指由依法獨立行使職權之成員組成之決策性機關，其所審議議案之案由、議程、決議內容及出席會議成員名單。」

[4] 行政程序法第 46 條第 2 項：「行政機關對前項之申請，除有下列情形之一者外，不得拒絕：
一、行政決定前之擬稿或其他準備作業文件。…..」

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.7.2.1 分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法、發展與實作一套適當的資訊標示與處置程序。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織、所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

類別：資訊公開

【案號：*D980102*】

公文承辦人姓名屬於限制公開或得不予公開之資訊

【案號：台中高等行政法院 *98* 年度訴字第 *23* 號】

焦點話題

原告向被告機關提出陳情書，申請被告 *94* 年○月○日府工使字第 *0940xxxxx* 號函等 *21* 件公文承辦人姓名，被告機關以公文承辦人姓名屬政府資訊公開法第 *18* 條第 *1* 項第 *3* 款之應限制公開或不予提供事項而予以駁復。原告不服，提起訴願仍未獲准，遂提起行政訴訟。

法院審理後認為承辦人姓名及其職位，既為行政決定作成前之內部準備文件，若非對公益有必要者，被告機關自得不予提供，況被告機關已於上開原告所稱 *21* 件公文中已載有電話足資聯絡及溝通，是以認定原告請求無理由。

重點摘要

1. 公文承辦人員姓名屬於行政決定前的擬稿及其他準備作業文件，不在應公開的範圍內。

2. 公務人員製作公文書，是以機關名義所為公法上意思表示，其法律效果歸屬於機關，公文承辦人不須單獨對外承擔機關公文的責任。

法律觀點

台中高等行政法院之所以駁回原告的請求，主要是認為行政機關對外為意思表示係以機關的名義為之，其對外公文所載承辦人既係以代號為之，則各該代號表徵之職務擔當人即屬行政機關作成意思決定前，內部單位之擬稿或其他準備作業，屬於政府資訊公開法第 *18* 條第 *3* 款「政府機關作成意思決定前，內部單位之擬稿或其他準備作業」之應限制公開或不予公開之資訊，僅在對公益有必要時始得公開或提供。

行政院為促進行政效率，於 *89* 年 8 月 *16* 日以台 *89* 秘字第 *24413* 號函修正之「文書處理手冊」增訂「承辦人員得於文稿中敘明聯絡方式」的規定，由各機關參照上開規定辦理，本件被告對於公文書上登載承辦人姓名或代號，自得予以裁量如何登載，況且被告已於 *21* 件公文中載有電話足資聯絡及溝通，因此認定原告請求無理由而駁回。

管理 *Tips*

在政府資訊公開法的規範下，政府機構應主動針對其所保有的資訊進行辨識，判斷資料是否需公開、公開方式(公報、網頁、申請等)，並依此建立相關書面處理程序，政府機構應於民眾提出申請後 *15* 日內為准駁的決定。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.7.2.1 分類指導綱要

資訊依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。

二、檔案法

類別：資訊公開

【案號：*D980201*】

國家機密檔案朝全面開放修法

【資料來源：中國時報 *98/08/09*】

焦點話題

研考會檔案局參考美、德國檔案規範後，已提出檔案法修正草案送行政院審查。研考會主委江宜樺表示，此次修正基於「全面開放」原則，修法將明定各部會除了「國家機密保護」和「特殊情形」外，應主動辦理機密檔案的解密，凡屆滿期限或逾 *30* 年機密的檔案都應公開。

檔案法自民國 *91* 年起施行至今，但 *94* 年《政府資訊公開法》公布後，兩法之間互有扞格且疊床架屋，因此修法鬆綁解套。

現行條文規定「國家檔案至遲應於 *30* 年內開放應用，有『特殊情形』者得經立法院同意延長期限」。修正後將在第 *23* 條中規範「特殊情形」，如「國家機密保護法」情報考量，或依法有保密義務者，如檔案內容涉及個人資料，開放應用有侵害個人隱私之虞者（但經當事人同意、當事人死亡後卅年者、涉及公益、或政府機關曾公開的檔案不在此限）及其他經立法院同意延長期限者。

重點摘要

1. 檔案法之修正本於政府資訊應主動公開之原則，更能保障人民知的權利。

2. 政府資訊之公開，仍應注意法律應保密之事項及保護個人隱私。

3. 應建立檔案管理辦法及流程，以遵循法律規定之保密期限。

法律觀點

為健全政府機關檔案管理，促進檔案開放與運用，發揮檔案功能，因此我國於 *88* 年 *12* 月 *15* 日制定公布檔案法。但經過數年實務運作，面臨機關檔案類型繁多，有因應調整管理方式之需求，且現行檔案銷毀作業缺乏分級審查制度，導致審查程序效益不彰。另政府資訊公開法已於 *94* 年公布施行，對於機關檔案應用的法律適用有待釐清，因此檔案法修正草案因應而生。

依現行檔案法的規定，機關檔案保存年限區分表均應報送檔案中央專責機關審核，且各機關檔案銷毀悉須經檔案中央專責機關審核，導致現行銷毀檔案效果不彰[1]。因此參考國外相關立法例，在此次修正草案採取建立機關檔案銷毀分級審查機制，以分階段管理方式，先經由檔案中央專責機關事前審核各機關檔案保存年限區分表，降低檔案遭致不當銷毀之風險[2]。次於檔案保存年限屆滿認有必要時，透過鑑定程序再次審定確保檔案價值，以為後續檔案存毀之依據[3]。另外審酌上級機關對所屬機關負監督責任，因此由上級機關審酌檔案銷毀事宜，更能強化分級審查制度，因此修正檔案法第 *14* 條之規定，建立分級審查機制[4]。因此，修正草案通過後，透過分級審查、分段管理之方式，應能更有效率進行檔案銷毀作業。

---

[1] 檔案法第 12 條：「定期保存之檔案未逾法定保存年限或未依法定程序，不得銷毀。
各機關銷毀檔案，應先制定銷毀計畫及銷毀之檔案目錄，送交檔案中央主管機關審核。
經檔案中央主管機關核准銷毀之檔案，必要時，應先經電子儲存，始得銷毀。
機關檔案保存年限及銷毀辦法，由檔案中央主管機關擬訂，報請行政院核定之。」

[2] 檔案法修正草案第 10 條第 2 項：「各機關應就其主管業務，依檔案中央專責機關訂定之機關共通性檔案保存年限基準及其他相關法令規定，編訂檔案保存年限區分表，送交檔案中央專責機關審核。修正時，亦同。」

[3] 檔案法修正草案第 11 條：「各機關有下列情形之一，應辦理檔案保存價值鑑定；檔案中央專責機關依第 18 條規定受贈、受託保管或收購之文件或資料認有必要者，亦同：
一、訂（修）定檔案保存年限區分表認有必要者。
二、辦理檔案移轉者。
三、辦理檔案銷毀認有必要者。
四、檔案年代久遠而難以判定其保存年限者。
五、檔案保存技術變更而有重新檢討保存年限之必要者。
六、其他經檔案中央專責機關指定者。」

[4] 檔案法修正草案第 14 條第 2 項：「各機關銷毀檔案，應依下列規定辦理：
一、中央三級以上機關、省政府、省諮議會、直轄市政府及所屬一級機關、縣（市）政府及直轄市、縣（市）議會，應報經檔案中央專責機關同意。
二、鄉(鎮、市)公所、鄉 (鎮、市)民代表會，應報經縣政府同意。
三、其他機關應報經上一級機關同意。」

另外，依現行檔案法的規定，國家檔案至遲應於 *30* 年內開放應用，除非有特殊情形，得在立法院的同意下，延長期限[5]。但對於特殊情況所指為何，並沒有相關規定，因此在實務運作上會發生困難，是以此次修正增加特殊情形之規定，包括「依法律有保密義務者」、「檔案內容涉及個人資料，其開放應用有侵害個人隱私之虞者」及「其他特殊情形經立法院同意延長期限者」[6]，讓法律適用上更加明確，且可以更加落實政府資訊公開之規定。

經過此次檔案法之修正，相信公務機關在執掌檔案管理時，能夠更有效率，且也更能確立政府資訊應予以公開的原則。未來若修法通過後，機關應建立檔案管理辦法及流程，以期遵循法律規定之保密期限。

管理 *Tips*

因為《政府資訊公開法》及《檔案法》的規定下，政府機構可再考量以下 2 個面向的管理機制：

1. 不可公開資訊的辨識：未來政府資訊將以公開為原則，惟涉及個人隱私或法律規範等特殊情事方不得公開，是以單位可在先行辨識其保有之資訊的保護等級應符合那些相關的法律，並依此對單位內所有資訊進行機密等級分類，以免公開不適宜的資訊，導致民眾訴願。

2. 公開的管道的管理：政府資訊的公開可分為被動及主動，被動係指民眾透過申請方式取得，而主動則是指單位透過刊物發行、文宣品或網站方式公開，在主動的部分，組織應建立適當的控管及核准程序，以避免不正確或不適當的訊息被公布。

[5] 檔案法第 22 條：「國家檔案至遲應於三十年內開放應用，其有特殊情形者，得經立法院同意，延長期限。」

[6] 檔案法修正草案第 23 條第 1 項：「國家檔案至遲應於三十年內開放應用。但有下列特殊情形者，得不開放應用或限制開放應用：
一、依法律有保密義務者。
二、檔案內容涉及個人資料，其開放應用有侵害個人隱私之虞者。但經當事人同意、涉及公益、或政府機關曾經公開之檔案者，不在此限。
三、其他特殊情形經立法院同意延長期限者。」

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.7.2.1 分類指導綱要

資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。

A.7.2.2 資訊標示與處置

應依照組織所採用的分類法、發展與實作一套適當的資訊標示與處置程序。

A.10.9.3 公眾可用的資訊

應保護公眾可用系統上可取得資訊的完整性,以防止未經授權的修改。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

參、資訊監察（*Monitors*）

一、通訊保障及監察法

類別：資訊監察

【案號：*M980101*】

司法院：依法監聽　掛線僅 *6* 萬

【資料來源：中央社 *98/10/02*】

焦點話題

總統馬英九上任後宣示杜絕非法監聽。司法院表示，監聽票改由法官核發後，監聽已由過去最多 *60* 多萬線，大幅降至僅約 *6* 萬，國安監聽件數也銳減一半。

報載「馬上台 *1* 年情治監聽有增無減」、「掛線人數延伸監聽變濫聽」後，引發各界關注。國安局還發布新聞稿表示，將協調法務部、國防部等單位共同成立專案並提出調查報告。

根據司法院提供的資料，在通訊監察新制實施前，曾有 *1* 個年度監聽案件達 *8* 萬 *8192* 件、掛線 *60* 萬 *8376* 線，最低的年度監聽數，監聽線也達 *16* 萬 *5000* 線。但在新制實施後，*97* 年監聽總件數為 *1* 萬 *5645* 件，總線數 *6* 萬 *945* 線，已大幅降低；國安監察案件，*96* 年全年 *59* 件，*97* 年法院只核准 *33* 件。

司法院刑事廳長劉令祺表示，監聽一線最多可達 *10* 人次，以此計算，過去最高峰時曾有約 *600* 萬人次遭監聽，確實相當嚴重，目前依法監聽線數大幅減少，人次已降為過去的 *1/10*，已兼顧人權與犯罪偵查的平衡面。

重點摘要

1. 人民秘密通訊自由是憲法保障的權利，不可以任意侵犯。

2. 「通訊保障及監察法」即是保護人民秘密通訊的自由，通訊監察必須按照法律規定程序才能夠進行。

法律觀點

依憲法第 *12* 條的規定，人民有秘密通訊的自由[1]，因此秘密通訊是人民憲法上的權利，除非有憲法列舉的情況，否則不可以法律限制[2]。基於公共利益的考量，國家必須透過通訊監察的方式來偵查犯罪，「通訊保障及監察法」即是為了保障人民秘密通訊自由不受到非法侵害，並確保國家安全及維護社會秩序而制定。

依照「通訊保障及監察法」第 *5* 條第 *1* 項之規定，有事實足以認定被告或者犯罪嫌疑人有該法該條所羅列之罪嫌，並危害國家安全或社會秩序情節重大，而有相當理由可信其通訊內容與本案有關，且不能或難以其他方法蒐集或調查證據者，可以發通訊監察書。由此可知，通訊監察書的核發具有一定的要件要求，若有其他方法可以蒐集或調查證據時，即不得以監聽通訊的方式來蒐集或調查證據，以確保人民的秘密通訊自由。另外，若有第 *6* 條所列的罪名，為防止他人生命、身體、財產之急迫危險，司法警察機關得報請檢察官以口頭通知執行機關先予執行通訊監察。但檢察官應告知執行機關第 *11* 條[3]所定之事項，並於 *24* 小時內陳報法院補發通訊監察書，若未能在時限內補發者，即應立即停止監察。

「通訊保障及監察法」於 *96* 年 *7* 月 *11* 日修法前，通訊保障監察書的核發機關是依照案件階段來核發，偵查階段由檢察官依司法警察聲請或職權核

[1] 中華民國憲法第 12 條：「人民有秘密通訊之自由。」

[2] 中華民國憲法第 23 條：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」

[3] 通訊保障及監察法第 11 條第 1 項：「通訊監察書應記載下列事項：
一、案由及涉嫌觸犯之法條。
二、監察對象。
三、監察通訊種類及號碼等足資識別之特徵。
四、受監察處所。
五、監察理由。
六、監察期間及方法。
七、聲請機關。
八、執行機關。
九、建置機關。」

發，審判中由法官依職權核發。因此檢察官於偵查階段可以核發通訊監察書。*96* 年 *7* 月 *11* 日修法後，通訊監察書一律改由法院核發，偵查階段的案件，由檢察官依司法警察的聲請或者依職權以書面載明理由並檢附文件向法院聲請核發，審判進行中，法官得依職權核發。是以透過法院的審查，可以更嚴格控管偵查階段通訊監察書核發狀況，以保護人民的秘密通訊自由，減少不必要的監聽。

在「通訊保障及監察法」修法以後，除事前審查機制外，違反該法者，也將面臨相關的民事及刑事責任。民事損害賠償部分，按監察通訊日數，以每一受監察人每日新台幣 *1000* 元以上 *5000* 元以下計算，若能證明損害高於該金額時，則不在此限[4]。公務員或委託執行公權力之人違法時，國家應負賠償責任[5]。刑事責任部分，最重將有 7 年以下有期徒刑之刑責[6]，應予注意。

管理 *Tips*

依「通訊保障及監察法」內針對執行監聽工作有相關嚴格之規範，包含申請程序、申請要件、監聽的執行及監聽所得資料的保存等等，組織應識別適法令中所需遵守的原則，並依此原則訂定相關作業程序，讓執行業務人員避免違反相關法律、法令，也應透過教育訓練及宣導，來使業務執行人員更清楚瞭解所應擔負之法律責任。組織也應考量並加強監聽紀錄及內容的保存及覆核，以確保合乎相關法律、法令之規範。具監聽所使用相關的設備與儀器也應適當的保存，以避免遭誤用或破解。

另外主管機構對需求提出單位也應有適當的宣導及解說，但應避免只單從規定的角度說明，而是要以可能造成個人資料外洩的風險說明，以增加需

[4] 通訊保障及監察法第 20 條：「前條之損害賠償總額，按其監察通訊日數，以每一受監察人每日新台幣一千元以上五千元以下計算。但能證明其所受之損害額高於該金額者，不在此限。
前項監察通訊日數不明者，以三十日計算。」

[5]通訊保障及監察法第 22 條：「公務員或受委託行使公權力之人，執行職務時違反本法或其他法律之規定監察他人通訊或洩漏、提供、使用監察通訊所得之資料者，國家應負損害賠償責任。
依前項規定請求國家賠償者，適用第十九條第二項、第三項及第二十條之規定。」

[6]參考通訊保障及監察法第 24 條至第 28 條。

求提出單位的瞭解及諒解。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.6.2.1 與外部團體相關的風險之識別

由涉及外部團體的營運過程產生對組織資訊及資訊處理設施之風險，應在核准外部團隊存取之前加以識別，並實作適當的控制措施。

A.6.2.2 處理客戶事務的安全說明

在賦予客戶存取組織資訊或資產的權限之前，應闡明所有已識別的安全要求。

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.7.3 資訊處置程序

應建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用。

A.10.10.2 監視系統的使用

應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。

A.13.2.3 證據的收集

在涉及法律行動(民事或刑事)的資訊安全事故後，對人員或組織的跟催措施，應收集、保存及呈現證據，以符合在相關審判時提出證據的規則。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.3 組織紀錄的保護

應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損及偽造。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

A.15.1.5 防止資訊處理設施的誤用

應制止使用者以未經授權的目的使用資訊處理設施。

A.15.3.2 資訊系統稽核工具的保護

應保護資訊系統稽核工具之存取，以防止任何可能的誤用或破解。

類別：資訊監察

【案號：*M980102*】

都是開心農場惹的禍？中研院監控同仁電腦！

【資料來源：自由時報 *98/11/19*】

焦點話題

人事行政局下令全國公務員不得利用上班時間玩網路遊戲，卻意外引爆，有些公務單位已經採買相關設備，監控個人電腦內的所有資訊，嚴重侵犯個人隱私。

立委指出，人事行政局對各公務機關發出公文，要求公務員不得在上班期間從事與公務無關之行為，特別是玩開心農場等網路遊戲。

然而中研院○○所所長卻在轉達相關公文時以手寫加註：「請轉告同仁，本所資訊室已增購全所各 *IP*、網際網路之監控器，必要時可查核辦公時間內之網路活動。」

立委質疑，行政機關可以假禁止網路遊戲之名，直接去監控公務員的電腦嗎？此舉已涉違反通訊保障及監察法、刑法妨害秘密罪各款，政府進行通訊監察，不得逾越必要之限度，且嚴重侵犯個人隱私。

中研院○○所所長解釋，這套設備是中研院計算中心同意他們添購的，平時並不會拿來監控同仁，只有出狀況時才會拿來查核。中研院院長則是表示添購監控設備，是為了資訊安全，加強防堵病毒，而不是要監控同仁上網，完全是誤會一場。

重點摘要

1. 監控網路活動涉及違反通訊保障及監察法，可能面臨 *5* 年以下有期徒刑之刑責。

2. 若事先得到被監查者的同意，可以不罰。

法律觀點

為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序，通訊保障及監察法因此誕生。因此，必須遵循該法相關規定，始可以進行通訊監察。

網路的活動及言論，屬於通訊保障及監察法第 *3* 條[1]第 *1* 項第 *1* 款「利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信」之通訊，且一般人對網路活動具有隱私或秘密的期待，是網路活動屬於通訊保障及監察法保護之範疇。

依照通訊保障及監察法的規定，受監察人涉及一定罪名，有相當理由可信其通訊內容與涉及案件有關，且不能或難以其他方法蒐集或調查證據時，經檢察官向法院聲請後發布通訊監察書。是以，一般公務機關是否對於機關同仁的網路活動進行監控？

依照通訊保障監察法第 *29* 條第 *3* 款[2]規定，若監察者已得到通訊一方同意，且非出於不法目的時，可以不罰。因此，若監控機關人員在取得機關人員事先同意下，是可以進行通訊監控。

所以通常為了避免有侵犯個人隱私權的疑慮，在公務機關已經公告說明，公務電腦應用於公務目的且不應進行個人通訊或其他隱私活動下，而為了保護公務機關的資訊通信安全而公告將進行資訊監控，應可認知已取得員工的默示同意。當然以書面或其他足資認定員工同意受監控的表示，是避

[1] 通訊保障及監察法第 3 條：「本法所稱通訊如下：
一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。
二、郵件及書信。
三、言論及談話。
前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。」

[2] 通訊保障及監察法第 29 條：「監察他人之通訊，而有下列情形之一者，不罰：
一、依法律規定而為者。
二、電信事業或郵政機關 (構) 人員基於提供公共電信或郵政服務之目的，而依有關法令執行者。
三、監察者為通訊之一方或已得通訊之一方事先同意，而非出於不法目的者。」

免爭議的作法，例如透過自然人憑證以線上方式簽署同意表示，即為一例。

管理 *Tips*

現今的網路世界資訊安全事件頻傳及因應網路異常事件的處理，越來越無法避免對資訊基礎建設(如網路、主機、資料庫)等存取或使用有所監控，是以就管理機制上，仍建議組織應有適當的機制告知員工被監控的狀況，而如需檢視監控資料時，則應有適當的核准及授權機制，並留存相關資料，以避免未有正當理由而侵犯個人隱私。以案例本身員工有反彈的情形，應可藉由教育訓練及宣導，讓使用者瞭解監控的必要性、資料保護狀況及被監控之狀況，以期能降低被影響人員的反彈。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A.10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

類別：資訊監察

【案號：*M980201*】

杜絕違法監聽　刑事局查扣抓姦機

【資料來源：聯合報 *98/03/10*】

焦點話題

馬總統上任後要求杜絕國內違法監聽行為，但最近有種未經 *NCC* 認證的「抓姦機」在徵信業爆紅。刑事警察局中部打擊犯罪中心逮捕違法業者 *OOO* 公司包括負責人等四人，該公司近幾年大量進口監聽器與針孔攝影機，轉賣給想捉姦、追蹤債務的客戶，他們在北部地區成立三家通訊門市，提供未經 *NCC* 認證的 *GSM* 監聽器，嫌犯 *OOO* 還自拍影音光碟，指導如何操作監視器、安裝針孔。

警方表示，*GSM* 監聽器體積只有半個香煙盒大，裝入手機 *SIM* 卡後安裝在車內，透過另一隻電話撥打 *SIM* 卡門號，監聽器即自動開啟，話筒會傳遞車內收錄的對話，並同步錄音。很多夫妻利用這套器材「抓猴」成功，這種監聽器除可收聽現場聲音，還可以接室內電話線，如果要錄音，可另在手機功能上設定。

「捉姦」監聽器雖隱密，被監控當事人不容易察覺，但市面上已有全頻掃描器，只要在周圍環境開啟，立即能掃描出機器訊號，或者追蹤針孔紅外線的訊號來源。

重點摘要

1. 電信管制射頻器材沒有經過國家通訊傳播委員會認證、審驗合格，不得製造、輸入、販賣或公開陳列，否則將違反電信法之規定。
2. 對於專用於電信處理之通信，不得以非法方法侵害他人的秘密，否則將依電信法之規定論罪。

3. 法律雖然保護配偶權以及財產權，但進行捉姦行為或追索債務時仍應以合法之手段行使權利，否則仍無法免責。

法律觀點

這個案例應分別就違法業者及使用者之角度來討論相關法律問題。案例中違法業者大量進口之 *GSM* 監聽器，是屬於電信管制射頻器材，依電信法[1]及電信管制射頻器材管理辦法[2]之規定，必須經過國家通訊傳播委員會[3]之認證、審驗後，才可以製造、輸入及販售，違反將被處新台幣(下同)*10* 萬元以上 *50* 萬元以下罰緩[4]。另外，依電信法第 *6* 條[5]之規定，電信事業及專用電信處理之通信，他人不得盜接、盜錄或其他非法方法之方法侵犯其秘密，違反者依電信法第 *56* 之 *1* 條[6]規定，將處 *5* 年以下有期徒刑，得併科 *150* 萬元以下罰金。此外，本案例 *GSM* 監聽器主要目的是用來監聽他人在車內或室內的談話並錄下來，乃是意圖營利提供工具或設備，便利他人以錄音方式竊錄他人非公開言論，同時也會違反刑法第 *315-2* 條第 *1* 項[7]之規定，刑責也是 5 年以下有期徒刑。

至於使用者購買 *GSM* 監聽器並用來進行監聽及錄音，除了同時違反上述電信法第 *6* 條及第 *56* 之 *1* 條之規定外，在刑法相關罪責的部份，主要是使用

[1] 電信法第 49 條第 3 項規定：「電信管制射頻器材非經型式認證、審驗合格，不得製造、輸入、販賣或公開陳列。但學術研究、科技研發或實（試）驗所為之製造、專供輸出、輸出後復運進口或經交通部核准者，不在此限。」

[2] 電信管制射頻器材管理辦法第 10 條規定：「電信管制射頻器材非經型式認證、審驗合格者，不得製造、輸入、販賣或公開陳列。但學術研究、科技研發或實（試）驗所為之製造、專供輸出、輸出後復運進口或經主管機關核准者，不在此限。」

[3]電信管制射頻器材管理辦法第 4 條規定：「本辦法之主管機關為國家通訊傳播委員會。」

[4] 電信法第 65 條第 1 項第 10 款規定：「有下列各款情形之一者，處新臺幣十萬元以上五十萬元以下罰鍰：…一○、違反第四十九條第三項規定，擅自製造、輸入、販賣或公開陳列未經型式認證、審驗合格之電信管制射頻器材者。」

[5] 電信法第 6 條第 1 項規定：「電信事業及專用電信處理之通信，他人不得盜接、盜錄或以其他非法之方法侵犯其秘密。」

[6] 電信法第 56-1 條規定：「違反第六條第一項規定侵犯他人通信秘密者，處五年以下有期徒刑，得併科新台幣一百五十萬元以下罰金。」

[7] 刑法第 315-2 條第 1 項：「意圖營利供給場所、工具或設備，便利他人為前條第一項之行為者，處五年以下有期徒刑、拘役或科或併科五萬元以下罰金。」

者的行為違反刑法第 *315-1* 條[8]有關竊錄他人非公開言論之規定，其刑度為處 *3* 年以下有期徒刑、拘役或 *3* 萬元以下罰金。另外，使用者之行為也有同時違反通訊保障及監察法第 *24* 條第 *1* 項[9]之虞，得處 *5* 年以下有期徒刑。

我國法律雖然保護配偶權以及財產權，但是進行捉姦或追索債權之動作仍應透過合法之方式進行，若行使權利的手段違反法律，除了要擔負刑責外，原來要達到的目的恐怕也無法實現，套句俗話，賠了夫人又折兵。

管理 Tips

本案例對業者及使用者而言同時均需針對其行為及銷售的貨品，清楚地辨識其所需遵遁的法令法規，特別針對個人資料的資料保護與隱私權的考量，更應有適當，以避免踰越了法律的規範。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A 15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A 15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

[8] 刑法第 315 之 1 條：「有下列行為之一者，處三年以下有期徒刑、拘役或三萬元以下罰金：
一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。
二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。」

[9] 通訊保障及監察法第 24 條第 1 項：「違法監察他人通訊者，處五年以下有期徒刑。」

肆、資訊應用（*Application*）

一、電子簽章法

類別：資訊應用

【案號：*A980101*】

貨櫃電子封條取代人工押運

【資料來源：中央社 *98/02/21*】

焦點話題

行政院經濟建設委員會表示，政府推動的「貨櫃電子封條監控系統」已於高雄港完成測試並正式啟用，可望使台灣貿易過程更安全與便捷，並帶來更多商機。經建會表示，未來高雄港押運的轉口櫃將加封電子封條，司機使用自然人憑證，即完成以科技取代人工押運轉口櫃的作業。

經建會表示，經高雄港運送的貨櫃，約有半數是轉口貨櫃，過去海關為防杜轉口櫃在運送途中遭掉包走私，針對高風險貨物採用人工押運方式監控，無形中增加人力及航商成本。為使高雄港轉口貨櫃以科技取代人工押運，因此推動「高雄港轉口櫃免押運計畫」，在經濟部技術處協助下，中科院、工研院及資策會等系統團隊合力開發，使相關技術獲突破。經建會表示成功建置貨櫃電子封條，不僅對海關押運及查緝更具功效，也可提升台灣經貿形象，未來擴大適用後，可為台灣帶來更多貿易商機。

重點摘要

1. *RFID* 技術廣泛應用在物流業，可以降低管控的人力成本及時間。
2. 以 *RFID* 傳輸資料必須做好加密措施，避免電子資料傳輸過程中造成資料外洩。
3. 自然人憑證具有加密功能以及身分鑑別性，可以確保資訊傳輸安全以及避免冒名的情況。

法律觀點

貨櫃電子封條乃是以無線射頻(*Radio Frequency Identification, RFID*)作成。*RFID* 可以說是電子標籤，它是由感應器及 *RFID* 標籤所組成，原理是利用感應器發射的無線電波，觸動感應範圍內的 *RFID* 標籤，藉由電磁感應產生電流，供應 *RFID* 標籤上的晶片運作並發出電磁波回應感應器。*RFID* 標籤上的晶片可以記錄資料，讓產品上的標籤可與周圍百公尺內的感應器溝通，而達到資料的交換及辨識。此項技術已經廣泛應用在物流業的運作，物流的每個流程，包含進貨、製造、出貨、上櫃、運送、通關等等，都可以透過 *RFID* 快速辨識商品的所有狀況，可以省去人工盤點及處理成本，因此使用電子封條避免轉口貨櫃被掉包，且可以加速貨櫃通關、減少航運成本並加強管理。

至於自然人憑證，在概念上具有網路身份證及網路印鑑的功能，透過電子簽章[1]及加解密機制可以達成辨識身分及確保資料完整性及隱密性，因此透過自然人憑證可以確認並辨識司機的身分，可以提高轉口貨櫃免押運計畫之安全性。

但應注意的是，*RFID* 標籤體積雖小，但其可以記錄許多資料，例如可以記載產品名稱、製造商、配銷地點...等，因而可以將需要的產品資訊寫入標籤內，以便進行管理。然而因為 *RFID* 讀取資料是透過無線電波傳輸，因此在傳輸過程可能會被第三人用其他讀取器攔截資料，若標籤上記載的是機密資料，就會有資料外洩的可能。其次，有心人士也有可能攔截資料後並竄改或刪減 *RFID* 標籤上記載的事項，讓讀取器接收到錯誤的資料。這些攔截或篡改刪減資料的動作都可以利用無線射頻的特性透過儀器輕易完成，反而讓競爭對手更容易進行探取商業機密或進行不當競爭，因此若 *RFID* 標籤記載事項涉及商業機密時，必須作好加密工作，並在使用目的後移除或

[1] 電子簽章法第 2 條第 2 款：「電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。」

銷毀，以保護商業機密。

我國目前沒有特別針對 *RFID* 制定專門法律規範，上述不法行為的類型，可以透過刑法[2]、電腦處理個人資料保護法[3]、營業秘密法[4]及民法[5]等相關法律來規範。

管理 *Tips*

對高雄港貨櫃站之管理單位而言可從以下幾個面向思考其資訊安全管理機制是否完善：

1. 對 *RFID* 所使用的範圍訂定實體安全防護周界，避免不明人士於周界中從事不當之行為。

2. 避免使用 *RFID* 傳輸機敏性資料，儘可能將機敏性資料均於伺服器端處理，僅用 *RFID* 傳輸貨物識別碼。如有必要傳輸也使用加密機制對資料進行加密後再傳輸。

3. 如為可更改資料的 *RFID* 標籤，則可定期針對使用範圍進行技術性掃瞄，以確認是否有不明的惡意訊號欲竄改 *RFID* 標籤上的資料。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.9.1.1 實體安全周界

應使用安全周界(諸如牆、卡控入口閘門或人員駐守的接待櫃檯等屏障)，以保護含有資訊及資訊處理設施的區域。

---

[2] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

[3] RFID 標籤若寫入資料為個人資料時，登記資本額 1000 萬元以上股份有限公司型態、採會員制之百貨公司或零售業，即有電腦處理個人資料保護法之適用。但是屬於銷售鏈前端的物流業，目前不是主管機關指定適用電腦處理個人資料保護法的行業，因此目前不受該法的規範。

[4] 若攔截的資料為營業秘密時，依營業秘密法第 10 條第 1 項第 1 款之規定，以不正當方法取得營業秘密者，為侵害營業秘密，並得依營業秘密法第 12 條之規定請求損害賠償。

[5] 行為人構成侵權行為時，並得依民法第 184 條侵權行為規定請求損害賠償。

A 10.8.4 電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A 12.3.1 使用密碼(加密)控制措施的政策

使用密碼控制措施以保護資訊的政策應加以發展與實作。

A 12.6.1 技術脆弱性控制

應取得關於使用中資訊系統之技術脆弱性的及時資訊、評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。

類別：資訊應用

【案號：*A980102*】

香港聯合醫院率先將病人資料上載至互聯網　減少遺失「手指」洩病歷

【資料來源：明報 *98/08/04*】

焦點話題

香港公立醫院接二連三發生醫護人員遺失載有病人隱私及病歷的 *USB* 事件。為了杜絕病人資料外洩問題，聯合醫院將率先引入全新的資料安全性措施，將病人資料上載至電腦伺服器，再安排每個醫護人員擁有一個帳戶和密碼，當他們在使用院外電腦時，只需要輸入用戶資料，就可以隨時閱覽病人病歷。九龍東醫院聯網總監陸志聰表示：「全部需要資料處理的同事都會用此方法，不會遺失 *USB* 手指的風險。」

陸志聰並表示，為安全性理由，建議醫護人員避免在伺服器的紀錄中，記載病人姓名及身分證號碼等個人資料，只以醫管局的病人編號來識別。若拿到病人編號，難以追查身分，拿到資料都沒有用。他並強調，系統會作多重保全，雖然難完全避免駭客入侵，但相信系統已相當安全。雖然新系統可能會有風險，例如遺失個人密碼，但始終比 *USB* 安全。

病人互助組織聯盟副主席張德喜認為，除了改善保全系統外，當局更應關注醫護人員的操守，提供培訓，讓他們懂得尊重病人隱私。

重點摘要

1. 涉及病人病歷及個人基本資料等隱私資訊，應該禁止醫護人員儲存至任何可攜式儲存設備及個人電腦，避免因設備遺失，或遭有心人士竊取，而造成資料外洩。

2. 將病人姓名及個人身分證資料以編號方式來識別，可以有效維護病人隱私，並確保資料外洩時的隱私安全。

3. 上傳到伺服器之資料，應配合使用醫事憑證進行加密，避免資料被駭客攔截而外洩。

法律觀點

依我國電腦處理個人資料保護法之規定，自然人的姓名、出生年月日、身分證統一編號、健康及病歷，均是屬於個人資料[1]，醫院亦屬於電腦處理個人資料保護法規範的非公務機關[2]，因此醫院必須向主管機關申請登記並取得執照，才可以進行個人資料的蒐集及電腦處理[3]。

目前醫療院所會將診療紀錄輸入至電腦裡儲存，一般都是以輸入帳號及密碼之方式作為控管使用權限之方式，因此只要能夠取得帳號及密碼時，任何人都可能在醫院電腦裡登入後取得資料。此外，如果醫院電腦沒有控制存取之情況下，相關人員即有可能將病歷儲存至可攜式儲存設備及個人電腦，增加病歷外洩的風險。而醫院若將病歷資料上傳至伺服器，在上傳過程中若未進行加密，資料可能會遭到駭客攔截，且以輸入帳號密碼作為存取權限的控管方式，將無法確認使用人員之身分，也有資料外洩之風險。

為了對外提供醫療電子認證服務及電子簽章機制，並在醫療體系內形成安全可信賴的醫療資訊交換環境，因此行政院衛生署設立了醫事憑證管理中心，針對醫療人員簽發醫事憑證，以應用在具風險之醫療專屬通訊網路或網際網路上、傳送敏感之醫療隱私資料。醫事人員憑證 *IC* 卡可以說是醫事人員之電子證照，可以識別使用者身份暨電子印鑑證明，並確保網路傳輸資料之安全性，減少病人敏感性資料外洩的風險，是以各大醫療院所如妥善利用醫事憑證之特性，可建立既便利又可維護病人隱私權之安全系統。

---

[1] 電腦處理個人資料保護法第 3 條第 1 款：「個人資料：指自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。」

[2] 電腦處理個人資料保護法第 3 條第 7 款：「非公務機關：指前款以外之左列事業、團體或個人：…
(二) **醫院**、學校、電信業、金融業、證券業、保險業及大眾傳播業。」

[3] 電腦處理個人資料保護法第 19 條第 1 項規定：「非公務機關未經目的事業主管機關依本法登記並發給執照者，不得為個人資料之蒐集、電腦處理或國際傳遞及利用。」

值得注意的是，除了存取權限的控管外，對於敏感個人資料，也應考慮如果外洩時，是否可以採取其他保護個人資料之措施。所以案例中以編碼方式處理個人識別資料，讓病歷資料外洩時，也無法知悉或識別個人資料，是有效防止隱私揭露的具體作法，值得我們學習。未來個人資料保護法草案通過後，若非公務機關代表人、管理人或其他有代表權人能證明已盡防止義務，可以避免被處以罰緩[4]。是以編碼方式處理個人資料，有助於保護個人資料，也可以免除或減低醫療機構可能面臨的賠償罰則或責任[5]。

管理 *Tips*

在本案例中香港聯合醫院所採用的機制，確實能有效降低透過 *USB* 外洩病歷的危險，惟仍可在以下幾個層面確認其控管的完整性：

1. 存取權限的授與，由於醫事人員可在非院內存取病歷，是否醫院更要清楚的訂立存取權限的授與，以避免醫事人員不當存取他人資料。

2. 使用者身份的確認，在國內已推行醫事人員憑證數年，是以可進一步利用醫事憑證來做為雙重身份認證，以加強其安全性。

3. 傳輸過程中的安全，也可利用醫事人員憑證上的金鑰，將傳輸中的資料進行加密。

存取紀錄的保存，由於醫事人員可在非院內存取病歷，且電子病歷只要外洩一筆便有其嚴重性，是以應針對每筆存取均有留有可識別性的 *log*，以利日後如有問題事後的追蹤。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

[4] 個人資料保護法草案第 49 條：「非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。」

[5] 例如，採行此措施可以主張依現行電腦處理個人資料保護法第 28 條但書即「非公務機關違反本法規定，致當事人權益受損害者，應負賠償責任。但能證明其無故意或過失者，不在此限。」

A.8.2.2 資訊安全認知、教育及訓練

組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。

A10.10.1 稽核存錄

稽核日誌係記錄使用者活動、異常及資訊安全事件，宜產生與保留一段議定的期間，以協助未來的調查與存取控制監視。

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A 11.3.1 通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

A.11.4.2 外部連線的使用者鑑別

應使用適當的鑑別方法，以控制遠端使用者的存取。

A.11.5.2 使用者識別與鑑別

所有使用者應有僅限其個人使用的唯一識別符(使用者 *ID*)，並應選擇適切的鑑別技術，以證實使用者宣稱之身分。

A 12.3.1 使用密碼(加密)控制措施的政策

使用密碼控制措施以保護資訊的政策應加以發展與實作。

A.13.2.3 證據的收集

在涉及法律行動(民事或刑事)的資訊安全事故後，對人員或組織的跟催措施，應收集、保存及呈現證據，以符合在相關審判時提出證據的規則。

類別：資訊應用

【案號：*A980103*】

考生遭冒填志願　大學分發擬採自然人憑證

【資料來源：自由時報 *98/08/09*】

焦點話題

大學考試入學分發放榜前，新竹高中彭姓學生疑因日常嫌隙，自掏腰包多花 *210* 元繳登記費，冒用身分為同班盛姓同學選填志願，但因只填了國立台灣大學醫學系一個志願，導致盛同學高分落榜，分發委員會表示，盛同學可以外加名額方式重新分發，分發會也會檢討志願登記流程。

大學考試現行的登記方式是考生繳款成功後，就可取得繳款帳號及考生通行碼，考生在開放登記志願時間內上網登入選填系統，利用身分證字號、指考准考證號碼、繳款帳號與通行碼四種號碼，才可選填志願。

受害學生父親認為，身分證字號在許多場合都會公開，准考證號碼則是考區試場與座位的編號，繳款帳號與通行碼也只要買一本分發資訊，「這四個號碼都不具密碼功能，也不能由考生變更」有違資訊安全的基本原則。

彭同學冒名填志願的事件，凸顯大學選填志願流程的資訊安全保護不足，大學分發會考慮改採「自然人憑證」方式，以確保學生權益。

重點摘要

1. 自然人憑證足以辨識使用者身份，可以避免身分被冒用。

2. 帳號密碼的設定，應該避免使用他人容易取得的資料，以確保資訊安全。

3. 個人應該妥善保管個人資料，避免被有心人士作為他用。

法律觀點

本案例涉嫌以盛姓學生身分證字號及指考准考證號碼，及購買分發資訊即

可取得的繳款帳號與通行碼，冒用盛姓學生名義登入大學考試入學分發網站選填志願，屬於無故輸入他人帳號密碼，入侵他人電腦及相關設備，可能會構成刑法第 358 條入侵電腦罪[1]，可能面臨 3 年以下有期徒刑之刑責。

在這個資訊化的時代，過去必須以人工處理的工作，現在都可以透過電腦來處理，不但可以節省人力、時間及成本，也可以提高事情處理的準確度。但是電腦的使用往往是透過輸入帳號及密碼來登入，只要能夠輸入正確的資料，就能夠登入系統並行後續作業，換言之，電腦是認帳號密碼，而不是認人，所以帳號密碼的安全性顯得非常重要。

此案例突顯帳號密碼安全性的問題。大學指考填選志願，必須輸入個人身分證字號、准考證號碼、繳款帳號及通行碼。前兩者是屬於個人資料，但身分證字號及准考證號碼均屬於容易取得的資料，至於繳款帳號及通行碼，只要購買分發資訊就可以取得，繳款帳號與通行碼並未與考生個人身分作連結，是以冒用身分填選志願並非難事。

為確保類似事件發生，的確可以慎重考慮以自然人憑證作為身分驗證的工具。自然人憑證相當於網路身份證，以自然人憑證作為個人身分確認工具，將是對於個人資料保護大幅度提升保護強度。而個人只須要妥善保管自然人憑證，就可以避免遭他人冒用，可以提高資訊的安全性，避免類似事件再度發生。不過應注意的是，自然人憑證目前申請核發年齡為 18 歲，對於未滿 18 歲之考生應如何處理，也是這個機制可以再考量或與自然人憑證管理中心協商的地方。

管理 Tips

就此案例而言，可從下面 3 個層面來檢視：

*1.*使用者申請註冊的程序：大考中心應再衡量於申請過程當中使用者所提出

[1] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

身分證明文件是否適當，是否僅為註冊者自己知曉或可取得之識別，若是透過網路申請，可於寄送准考證或成績單之時另付一識別碼或密碼或使用自然人憑證註冊，均可加強身份之識別。

2.使用者登入程序：應考量更能確認使用者身分之登入驗證機制，可同第 1 點採用自然人憑證做為身分識別之方式，惟此案例中係從註冊時即為冒名註冊，此部分做法較無法預防上述案例，但因注意。

3. 使用者個人資料之保存：使用者應於平日即多注意個人資料之保存與使用，如身分證字號、生日及電話，以免遭有心人士利用，另密碼的選用也應避免採用以上的資訊。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.11.2.1 使用者註冊

應有適當的正式使用者註冊與註銷註冊程序，以對所有資訊系統與服務核准和撤銷存取。

A.11.3.1 通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

A.11.5.2 使用者識別與鑑別

所有使用者應有僅限其個人使用的唯一識別符(使用者 ID)，並應選擇適切的鑑別技術，以證實使用者宣稱之身分。

類別：資訊應用

【案號：*A980104*】

推廣工商憑證　經部估 98 年底達 92 萬張

【資料來源：中央社 *98/09/27*】

焦點話題

經濟部為協助企業降低成本，將投入新台幣 7 億元發給企業工商憑證，預估 *98* 年底可望達 *92* 萬張。經濟部在 *92* 年就開始推廣工商憑證，原意是協助公司行號降低成本、減少開銷，企業可以付費申請，不過企業興趣不高，至今年上半年僅約共發出 *30* 萬張，經濟部決定利用政府振興經濟擴大公共建設預算經費，支出約 *7* 億元擴大發出工商憑證。

經濟部預估，國內共 *133* 萬家企業中，*92* 萬家也就是約 *7* 成企業都將擁有工商憑證；而收到工商憑證應用包的公司商號，可以馬上體驗超過 *29* 項電子化政府的應用機制，包括報稅、工商登記、勞健保加退、電子發票等服務。

重點摘要

1. 工商憑證是企業的網路身份證明及電子印鑑，可以直接在線上使用電子化政府的應用機制，降低書面申請及臨櫃辦理須花費的費用及時間成本。
2. 企業領取工商憑證後，可使用正卡申請多張附卡，讓多位員工分工使用。惟對於附卡可以使用的業務範圍，企業必須做好內部權限控管，避免無權使用之風險。

法律觀點

隨著數位時代的來臨，為提供更迅速便民的服務，行政院研考會近幾年來不斷推動電子化政府的發展，以提高行政效能，創新政府的服務，提升便民服務的品質，以達到讓企業、社會大眾可以在任何時間及地點，以多種管道獲得便利的服務。

網路上進行的活動，重點在於如何確認行為人的身分，工商憑證即是企業的網路身份證明及電子印鑑。有別於自然人憑證是由個人自行保管的特性，企業因為業務多元，有多項業務共同使用一張工商憑證，常有無法符合業務運作需求的情形。為因應多個應用系統及多位承辦人員使用，減少卡片共用以及企業負責人保管工商憑證的疑慮，方便公司行號內部作有效控管及權責區分，可以使用正卡在線上申請多張附卡。因此，公司行號可以透過附卡的申請，使企業內部其他業務主管人員或其授權之人，基於業務工作需求，於業務範圍內使用附卡代表企業。

工商憑證目前已能使用在工商登記、領投標、報稅、勞保加退保等電子化政府應用，使得公司行號進行申辦時，可以不受限於收件時間及地點。此外，，除了電子化政府的相關應用外，憑證也可以使用在其他電子商務的網路交易，可以帶給企業更多便利。但應注意的是，因為工商憑證具有身分識別的效果，若未妥善保管正卡及附卡，並且明確劃分權責的情況下，若遭企業內部人員逾越授權使用時，企業對於外部交易還是會有法律責任。因此，在享受網路時代便利的同時，也要注意企業內部的權責管控問題，避免帶來法律風險。

管理 *Tips*

憑證的使用為數位環境證明持有者身分及簽署數位文件之用，故工商憑證的使用如同公司章一樣，具有相同法律的效力，是以就憑證的保管與使用管理對企業仍是首要必需考量之事。

對工商憑證而言，必須納入考量的部分則包含了：正卡與附卡的實體卡片，使用卡片時所需鍵入密碼的持有、保存及憑證使用的授權等，均應有妥適的規劃，以期能避免憑證遭盜用時所遭致的損失。

而對憑證維運的機構及權責單位而言，則應對憑證卡片的製發、展期、變更及終止，均有適當的管控，另有關憑證所能使用的服務，也應有適當的

管道告知持有者，最好也讓持有者有權利決定是否需使用該服務，以降低可能遭致損失的風險。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.11.2.1 使用者註冊

應有適當的正式使用者註冊與註銷註冊程序，以對所有資訊系統與服務核准和撤銷存取。

A.11.3.1 通行碼的使用

應要求使用者遵照良好安全實務去選擇與使用通行碼。

A.11.4.2 外部連線的使用者鑑別

應使用適當的鑑別方式，以控制遠端使用者的存取。

A.12.3.2 金鑰管理

應備妥適當的金鑰管理，以支援組織使用密碼技術。

類別：資訊應用

【案號：*A980105*】

衛生署加速實施電子病歷

【資料來源：中央社 *98/10/12*】

焦點話題

行政院經建會通過衛生署電子病歷計畫，預計 *3* 年後，國內 *8* 成醫院將提供影像、檢查等電子病歷，*6* 成醫院可以院際互通電子病歷，可縮短民眾看病等候時間、避免重複檢查。

衛生署表示，國內於民國 *94* 年就有電子病歷法源，但因誘因不足、經費有限等因素，電子病歷仍不普及，為減少重複檢查及用藥、縮短民眾看病等候時間、讓民眾享受持續性醫療照護，因此規劃「加速醫療院所實施電子病歷系統」子計畫。

衛生署預計至民國 *101* 年時，全國醫院實施電子病歷比例要達 *80%*、*400* 家，可提供跨院查詢電子病歷的醫院比例則要達至少 *6* 成，約 *300* 家。

衛生署並指出，一旦電子病歷實施普及，未來病人可在任一家醫院，透過健保 *IC* 卡，在病人同意及醫師授權下，就可完整取得病人過去的病史資料，提供連續性照護，希望在民國 *103* 年達成醫療機構全面實施電子病歷、病歷交換系統。

重點摘要

1. 電子病歷依法應簽名或蓋章時，須以電子簽章為之。
2. 病歷資料屬於敏感性資料，在電子病歷交換時，應取得當事人同意，避免產生糾紛。

法律觀點

依照醫療法的規定，醫療人員執行職務時，必須製作病歷並親自簽名蓋章，

且病歷的保存時間至少 7 年[1]，基於此保存義務要求，醫療院所必須準備適當的處所保存病歷，不但耗費空間，且在調取病歷的過程也將耗費些許時間。另外，病人若同時在不同醫院就診，因為就診資料無法流通，可能會因重複進行相同的檢查而浪費醫療資源外，也讓病人難以進行持續性的治療，因此電子病歷的實施及交換，即有其必要性。

醫療機構以電子文件方式製作及貯存之病歷，符合醫療機構電子病歷製作及管理辦法(以下簡稱電子病歷製作辦法)之規定時，可以免於製作書面病歷[2]。且依電子病歷製作辦法第 4 條之規定，電子病歷依醫療法第 68 條規定所為的簽名或蓋章，應以電子簽章的方式為之。如此一來，該電子簽章即醫事憑證可以確認製作病歷的醫療人員身分，且對於增加或刪除病歷時，也可以留下相關的紀錄。

電子病歷製作辦法沒有特別對電子病歷交換為相關規定。醫院是現行電腦處理個人資料保護法的規範對象，因此原則上只能在特定目的範圍內使用電子病歷。病歷製作的目的在於記錄醫療過程，提供給其他醫院應屬特定目的外之使用，因此除非病人自行申請病歷後提供給其他醫療院所，否則若是直接由醫院將電子病歷提供給其他醫療院所時，應經過當事人的書面同意。另外個人資料保護法草案針對醫療、基因、性生活、健康檢查等敏感性資料有特別規定，除非有列舉之例外情況，否則不得蒐集、處理或利用[3]，若違反規定時，將面臨 2 年以下有期徒刑，意圖營利者，將面臨 5 年

[1] 醫療法第 70 條第 1 項：「醫療機構之病歷，應指定適當場所及人員保管，並至少保存七年。但未成年者之病歷，至少應保存至其成年後七年；人體試驗之病歷，應永久保存。」

[2] 醫療機構電子病歷製作及管理辦法：「醫療機構以電子文件方式製作及貯存之病歷（以下簡稱電子病歷），符合本辦法之規定者，得免另以書面方式製作。」

[3] 個人資料保護法草案第 6 條：「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：
一、法律明文規定。
二、法律未明文禁止蒐集、處理或利用，且經當事人書面同意。
三、公務機關執行法定職務或非公務機關履行法定義務所必要。
四、當事人自行公開或其他已合法公開之個人資料。
五、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料

以下有期徒刑[4]。因此，未來在病歷的蒐集、利用及處理時，應該更特別注意作業流程，以免觸法。

管理 *Tips*

隨著電子病歷的推廣，醫療機構應更進一步辨識所需適用的相關法令法規，並依此針對電子病歷的蒐集、利用及處理流程，確認其符合相關的規範。另針對交換時電子病歷於傳輸過程中的安全性更應有適當的保護措施，尤以相關應用系統開發時也應考量加密技術的採用。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.10.8.4 電子傳訊

電子傳訊涉及的資訊應適當地加以保護。

A.12.3.1 使用密碼控制措施的政策

使用密碼控制措施以保護資訊的政策應加以發展與實作。

A.15.1.1 識別適用之法條

對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之作法，宜加以明確界定、文件化及維持最新。

A.15.1.4 個人資訊的資料保護與隱私

應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。

經過處理後或依其揭露方式無從識別特定當事人。」

[4] 個人資料保護法草案第 40 條：「違反第 6 條、第 15 條、第 16 條、第 19 條、第 20 條第 1 項規定，或中央目的事業主管機關依第 21 條限制國際傳輸之命令或處分，足生損害於他人者，處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。

意圖營利犯前項之罪者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。」

類別：資訊應用

【案號：*A980106*】

黑道介入法拍屋　司法院擬修法防範

【資料來源：中央社 *98/11/13*】

焦點話題

法院傳出法拍屋因為黑道介入而廢標的案例。標的物是位於台北市民生東路的一處國宅及地下停車位，底價遠低於市價行情，相當熱門。但有意投標者看屋時，當場就被警告「不要亂買喔」！此標的物首次開標時，謝姓女子得標，卻有黑衣人到法院跟監投標者，司法事務官宣布謝女得標，*3* 度唱名時，謝女卻因黑衣人在場而不敢舉手「應標」，因而被視為棄權，司法事務官改宣布由價差約 *1* 百萬元的第 *2* 順位洪某得標。幸好，台北地院民事執行處庭長察覺有異，當場以有「外力」介入、當事人非自由意志而不應標、程序不合法為由，宣布「廢標」，創下國內首例。

同一標的物重新開標，台北地院與警方破天荒合作，動員 *45* 名警力，*6* 台攝影機，上回棄標並說「我怕死了」的謝姓女子，這次終於以 *3868* 萬元得標，比上次多花了 *468* 萬元。儘管大陣仗動員，但上次投標時的「黑衣人」，竟然混在人群中，似有恃無恐，警方已一一錄影蒐證；得標的謝女未到場，而委由代理人投標，警方事後層層保護，將代理人護送回家。

司法院高度重視此案，已研究將來是否採「網路法拍」或「通訊法拍」方式進行，另對於黑道干擾法拍，司法院也正研議，在「強制執行法」中新增訂「投開標擾亂罪」，對干擾強制進行者最重處 *5* 年徒刑或採取必要的留置等處分。

重點摘要

1. 透過網路法拍，除能解決黑道圍標的問題外，也可以節省人力及時間成本。
2. 網路法拍的制度須包括身份確認、投標書之書面要求、網路傳輸資料安全性問題、保證金繳納問題及線上開標程序，對於這些制度需求，電子簽章法及強制執行法的整合為重要規範基礎。

法律觀點

依現行強制執行法的規定，不論是動產或是不動產，都是採取現場投標的方式。有意投標者必須在特定期日，親自或委託代理人到場，由於投標與開標時間過於集中，因此產生黑道圍標的問題。

司法院研擬的網路法拍應可以解決上述問題。投標人可以透過網路投標，不必親自跑法院，因此可以增加投標人數，並提高標的物的拍定價格。且可以延長網路投標時間，大大降低黑道圍標的風險。因此，網路法拍可以解決目前法拍所面臨的問題。

依照強制執行法規定進行的拍賣程序，法院必須先公告相關事項[1]，法院可以酌定保證金額，命投標者於開標前繳納之[2]。投標者之

[1] 強制執行法第 81 條：「拍賣不動產，應由執行法院先期公告。
前項公告，應載明左列事項：
一、不動產之所在地、種類、實際狀況、占有使用情形及其應記明之事項。
二、拍賣之原因、日期及場所。如以投標方法拍賣者，其開標之日時及場所，定有保證金額者，其金額。
三、拍賣最低價額。
四、交付價金之期限。
五、閱覽查封筆錄之處所及日、時。
六、定有應買資格或條件者，其資格或條件。
七、拍賣後不點交者，其原因。
八、定有應買人察看拍賣物之日、時者，其日、時。」

[2] 強制執行法第 86 條：「以投標方法拍賣不動產時，執行法院得酌定保證金額，命投標人於開標前繳納之。」

投標書應以書件密封後投入票匭[3]。開標時由法官當場開示並朗讀之，若出現最高出價相同時，以當場增加金額最高者為得標者，無人增加價額，則以抽籤決定[4]。因此，網路法拍制度的設計，必須包括投標者身分確認、投標書之書面要求、網路傳輸資料安全性問題、保證金繳納問題及開標程序。

網路投標的程序可以透過使用數位簽章的電子憑證來完成，例如自然人憑證或工商憑證。此種憑證可以確認投標人身分外，並可確保傳輸資料完整性與安全性，在符合電子簽章法第 *4* 條第 *2* 項[5]規定下並得將電子文件等同於書面文件。至於保證金的部份，則必須搭配網路銀行等相關機制作為對應，以確保保證金到位。至於開標時若遇到最高投標價格相同時，則可由投標者使用憑證在線上進行出價，以決定得標者。

網路法拍可以解決目前現場投標的缺點，但在擬定相關制度時，對程序必須有周延的設計，以確保網路法拍的公正性及正確性。

管理 Tips

採用「網路法拍」的確可提高拍賣之效率、降低需投入的人力與時間成本，並避免惡意威脅的發生，但也因為少了實體的身分驗證，可能導致詐騙、冒名之類的事件發生機率提高，是以如欲採用「網路法拍」應加強考量完整嚴謹的整體權限授與及身分驗證機制，包

[3] 強制執行法第 87 條：「投標人應以書件密封，投入執行法院所設之標匭。
前項書件，應載明左列事項：
一、投標人之姓名、年齡及住址。
二、願買之不動產。
三、願出之價額。」

[4] 強制執行法第 90 條第 1 項：「投標人願出之最高價額相同者，以當場增加之金額最高者為得標人；無人增加價額者，以抽籤定其得標人。」

[5] 電子簽章法第 4 條第 2 項：「依法令規定應以書面為之者，如其內容可完整呈現，並可於日後取出供查驗者，經相對人同意，得以電子文件為之。」

含了從使用者帳號申請/授與的政策、帳號的申請、身分的驗證、帳號的使用與追蹤等均需有適當的考量，另也由於非實體交易的屬性，需考量電子文件的效力及網路傳輸的加密機制，前者可考量引用「電子簽章法」之規範，採用適合之憑證，後者則可考量現行網路常用之加密機制如 *SSL*、*SET* 等以確保傳輸過程之安全性。

相關標準

CNS 27001 資訊技術-安全技術-資訊安全-管理系統-要求事項

A.11.1.1 存取控制政策

應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。

A.11.2.1 使用者註冊

應有適當的正式使用者註冊與註銷註冊程序，以對所有資訊系統與服務核准和撤銷存取。

A.12.3.1 使用密碼(加密)控制措施的政策

使用密碼(加密)控制措施以保護資訊的政策應加以發展與實作。